SNA-30

LANDSAT 7 DATA HANDLING FACILITY

EDC Landsat 7 DHF Network System Description

Revision 1
April 2000

United States Geological Survey
Earth Resources Observation Systems (EROS) Data Center
Sioux Falls, South Dakota

EDC Data Handling Facility Network System Description

Prepared by:

_____

Kimberly S. Johnson, Systems Engineer
Landsat 7 Data Handling Facility
Raytheon ITSS
USGS/EDC

Concurrence by:

_____

Barry Eberhard, DHF Manager
Landsat 7 Data Handling Facility
Raytheon ITSS
USGS/EDC

Approved by:

_____

R. J. Thompson
Landsat 7 Program Manager
USGS/EDC

Preface

This document is under the control of the Landsat 7 Data Handling Facility (DHF) Configuration Control Board (DCCB).

Configuration Change Requests (CCRs) to this document, as well as supportive material justifying the proposed changes, should be submitted to the L7 DHF DCCB.

Abstract

The EROS Data Center Network System Description for the Landsat 7 Data Handling Facility (DHF) describes the network design connecting the Landsat 7 Ground Station, Landsat 7 Processing System, and the Landsat 7 Image Assessment System. These systems

Facility (DHF) describes the network design connecting the Landsat 7 Ground Station, the Landsat 7 Processing System, and the Landsat 7 Image Assessment System. These systems

are resident at the EROS Data Center (EDC) in Sioux Falls, South Dakota. The Landsat 7 network's functional design, system architecture, external interfaces, and the manner in which the system will be operated (post-launch) at EDC in described in this document.

Table of Contents

Section 1 Introduction

1.1 Purpose

This document describes the network design for the Landsat 7 Data Handling Facility (DHF) at the EROS Data Center (EDC) in Sioux Falls, South Dakota. The Landsat 7 network's functional design, system architecture, external interfaces and the manner in which the system will be operated at EDC will be discussed.

1.2 Scope

This document describes all aspects of the Landsat 7 Network System at the DHF including design strategies, network diagrams, hardware specifications, policies, agreements and software.

1.3 Document Organization and Contents

This document contains four sections:

Section 1 is the introduction to this document.
Section 2 describes the existing EDC Network.
Section 3 describes the Landsat 7 Network design and how it fits into the EDC Network.
This includes:
A brief history
The security implications of some Landsat 7 features
Data transfer requirements
A brief description of the network equipment
Software associated with this network
Network Policies
Interfaces with other entities
Section 4 contains the appendices

1.4 Roles and Responsibilities

Many groups are involved in defining and creating the network which will serve the needs of Landsat 7. First, there are the elements of the Data Handling Facility (DHF), the Landsat 7 Ground Station (LGS), the Landsat 7 Processing System (LPS), the Image Assessment System (IAS) and the DHF Management Organization (DMO). Then there are external organizations including the EDC Distributed Active Archive Center (DAAC), EOSDIS Core System (ECS), and the Mission Operations Center (MOC). There are also internal EDC groups with interests in the network: the Computer Services Branch (CSB) Network Team, which is responsible for maintaining it and the NASA Integrated Service Network (NISN) provides network services.

maintains part of the system and will retain some control over the network. Service providers, such as MCI, provide communication capabilities on demand. These will each be discussed in more detail in the following paragraphs.

1.4.1 Landsat 7 Ground Station (LGS)

The LGS developers are responsible for providing the Ground Station systems for Landsat 7. This includes the antenna, RF equipment, Radome and controlling hardware and software for X-band and S-band. Due to the transmission and receipt of S-band data (the command and control data), LGS requires a higher level of network security than the other Landsat 7 elements. LGS connects to the LPS via dedicated hard-lines. These do not pose a network security risk. The LGS also connects to the MOC to receive Contact Schedules and Station Acquisition Data. From a network perspective, the LGS is separate from both the DHF and the EDC networks. All LGS network connections are made via closed network (MODnet) to the MOC. Refer to Figure 1 for further details.

1.4.2 Landsat 7 Processing System (LPS)

The LPS developers are responsible for providing the Level 0 processing capabilities for Landsat 7. Currently, the LPS system includes five Challenge XL computers connected by FDDI ring to the EBnet router. The production end of EDC DAAC system is reached through this router. The LPS portion of the FDDI ring is only used for transferring scientific data (Level 0R data) through the EBnet router to the EDC DAAC. IP routing is disabled on the SGI computers to prevent them from acting as routers, which would create multiple paths through the network. The IP routing is disabled for performance reasons, but this also serves to create a more secure system. The LPS requires a daily Contact Schedule from the MOC and an NTP connection to an EDC provided server. The LPS also requires a Calibration Parameter File from IAS (nominally once per quarter). The direct connection to IAS poses no security risk, however, the connection via Internet to the MOC opens the DHF network to the outside world. LPS requires a less stringent level of security than LGS, since LPS has processing, but not command and control responsibilities. Refer to Figure 1 for further details.

1.4.3 Landsat 7 Image Assessment System (IAS)

The IAS developers are responsible for providing the Image Assessment System for Landsat 7. IAS includes three large computers and two analyst workstations connected by FDDI ring to the EDC Campus router and then through the ECS router to the user end of the ECS system. The FDDI ring is used for scientific data transfer. IP routing is disabled on the SGI computers, which comprise the data processing side of IAS. The same rationale that applies to LPS FDDI applies here, although this will have no impact on network security. In addition to the image data from the EDC DAAC, the IAS requires certain statistical information from the DAAC and timing data from the Naval Research Laboratory. The IAS sends Calibration Parameter files to the MOC, LPS, and the EDC DAAC. These requirements will be met by direct connections to the other Landsat 7 elements and via Internet to the MOC and Naval Research Laboratories. IAS requires a less stringent level of network security than either LGS or LPS since IAS does off-line processing only. Refer to Figure 1 for further details.

1.4.4 DHF Management Office

The DMO is the managing entity of the DHF. It is primarily interested in access to management information via the network. Although the amount of data transmitted is small, from a network standpoint, a connection is required from the DMO's office equipment to the Problem Tracking System, CM System, and QA databases. Additionally, reports from the other DHF organizations must get to the DMO and the daily and weekly schedules must get to the operators.

1.4.5 EOSDIS Core System (ECS)

Refer to Figure 2. The ECS system is resident in the EDC DAAC (Distributed Active Archive Center). The ECS is responsible for providing the capability to store and retrieve large amounts of data for the EDC DAAC, including Landsat 7 data. Landsat 7 DHF connects to ECS in two places. LPS provides Level 0R data via the EBnet routers to the production end of ECS (the ingest servers on the diagram). IAS retrieves data, in a modified format, from the user end (the ECS router on the diagram). The ECS influences the Landsat 7 network design due to design limitations at both ends of the ECS network. ECS also has different security requirements than Landsat 7.

1.4.6 Mission Operations Center (MOC)

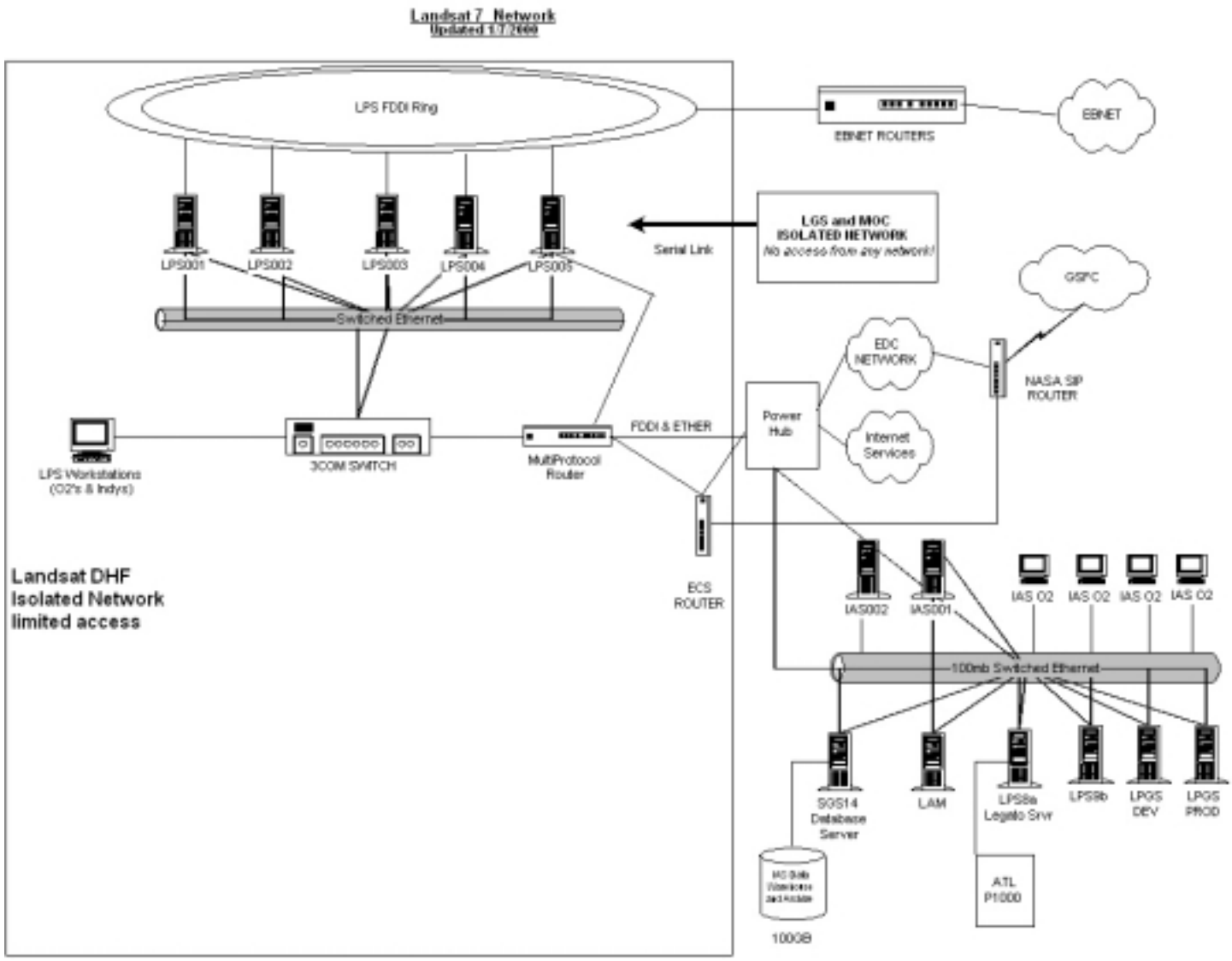
The MOC incorporates data from many sources including weather information, Landsat 7 information, orbital characteristics and user requirements into a single, daily schedule - the Contact Schedule (for LGS and LPS) and Station Acquisition Data (for LGS). The MOC also provides Definitive Ephemeris to IAS. The MOC has both a closed segment and an open segment connection to the Landsat 7 equipment at EDC. The current MOC hardware design is not critical to this document.

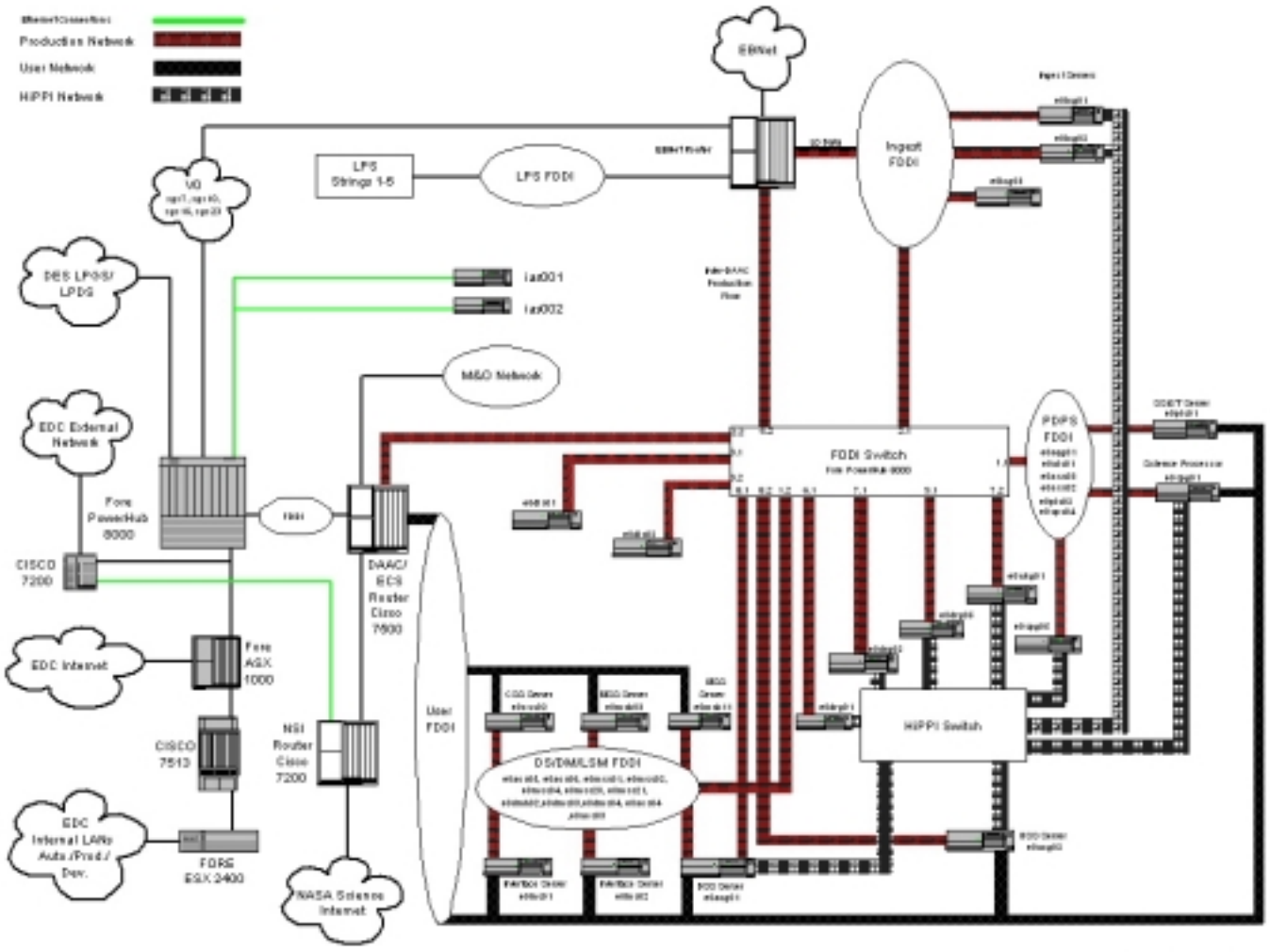
1.4.7 EDC Computer Services Branch (CSB)

CSB is responsible for computer, network and system administration expertise and maintenance at EDC. After Landsat 7 transition to EDC, this will include the DHF systems.

1.4.8 NASA Integrated Support Network (NISN)

NISN retains control and maintenance responsibility for the EBnet and MODnet routers installed at EDC. NISN requires a self-certification of security and a NISN audit of any organizations that hook up to the EBnet or MODnet. The self-certification includes network diagram, security policies and a checklist of 34 security-related items.


Landsat 7 Network
Updated 1/7/2000
LPS FDDI Ring
EBNET ROUTERS
EBNET
LPS001
LPS002
LPS003
LPS004
LPS005
Serial Link
LGS and MOC
ISOLATED NETWORK
No access from any network!
Switched Ethernet
GSFC
EDC
NETWORK
NASA SIP
ROUTER
Power
Hub
Internet
Services
FDDI & ETHER
LPS Workstations
(O2's & Indys)
3COM SWITCH
MultiProtocol
Router
ECS
ROUTER
Landsat DHF
Isolated Network
limited access
IAS002
IAS001
IAS O2
IAS O2
IAS O2
IAS O2
100mb Switched Ethernet
SGS14
Database
Server
LAM
LPS8a
Legato Srvr
LPS8b
LPGS
DEV
LPGS
PROD
ATL
P1000
100GB


Production Network
User Network
HIPPI Network
EBNet
LPS Strings 1-5
LPS FDDI
I/O
Ingest FDDI
DES LPGS/ LPDS
ias001
ias002
M&O Network
EDC External Network
Foreg PowerHub 8000
fddi
DAAC/ ECS Router Cisco 7500
FDDI Switch
PDPS FDDI
CISCO 7200
EDC Internet
Foreg AGX 1000
CISCO 7513
NSI Router Cisco 7200
User FDDI
HIPPI Switch
DS/DM/LSM FDDI
EDC Internal LANs Auto./Prod./ Dev.
FORE ESX 2400
NASA Science Internet

CRM 10/22/99

1.4.10 AT&T or SPRINT

AT&T or SPRINT provide telecommunications services to the EDC. They are not typically involved in the network design, they furnish bandwidth on request.

1.5 Network Terminology

Although there is an acronym list and table of definitions in the appendix, some understanding of network terminology is vital to the latter sections of this document. The following paragraphs are intended to clarify some of the terminology regarding networks and network hardware prior to discussion.

1. Network - the combination of hardware and cables which connect the computers of the various elements together.
2. Data Transfer Rates - bps = bits per second, Kbps = Kilo-bps (thousands of bits per second), Mbps = Mega-bps (millions of bits per second).
3. Router - For the purposes of this document, routers are devices used to connect two or more IP networks usually based on different LAN technologies, e.g., FDDI to 10 BaseT Ethernet and add some level of security or at least control at the packet level.
4. Concentrator - a device which connects the network interfaces of multiple machines to the network at the Media Access Control level.
5. Hub - a concentrator which connects a number of Ethernet interfaces to a network.
6. Interconnected - two computers are said to be interconnected if they can exchange information electronically via cable.
7. LAN - Local Area Network - the L7 Network hooked to and therefore part of the EDC Exchange LAN.
8. WAN - Wide Area Network - the L7 Network is hooked to the EBnet and the MODnet which are WANs.
9. T1, T3 and OC3 lines -the data rate of a T1 line is 1.544 Mbps, the data rate of a T3 line is 44.736 Mbps (45 Mbps). Optical Carrier (OC) lines are high-speed fiber optic transmission systems, an OC3 line has a data rate of 155.52 Mbps (155 Mbps).
10. Ethernet - LAN standard based on the ability for network devices to share a common wire by detecting when their signal "collides" with others to allow only one device to use the wire at a time. This technology, while cheap and easy to implement, is inherently inefficient, providing usually no more than 35% of its signaling rate in real data throughput on nominally loaded networks.
11. Internet - Refers to the worldwide public IP network infrastructure that links hundreds of thousands of universities, companies, and other organizations. Also known, not quite accurately, as the worldwide web. Internet is used in this document to mean any traffic that is transmitted over telecommunications channels that are not controlled by NISN.
12. Pipe is slang for the network cable/system. The size of the pipe refers to the signaling rate of the network media in bps, e.g. Ethernet is either 10Mbps or 100Mbps, FDDI is 100Mbps, etc. The pipe size is misleading in that it ignores overhead and transfer method, both of which vary widely and can be a significant fraction of this value. For example, with Ethernet, the bandwidth decreases logarithmically with the number of computers. Therefore, the actual data transfer rate may be 1 Mbps. For FDDI, each

computers has a time slot to transmit, so the data transfer rate may be as high as 80 Mbps.

13. Types of physical links:

ThinNet is coax cable (or in some instances twisted-pair) which connects to computers via standard BNC connectors which are normally "T"ed to provide a "daisy-chain" arrangement. The cables are small, flexible and the system can sustain a data rate of about 10 Mbps 10Base2: also known as ThinWire or Thin Ethernet, 10 Mbps, uses RG58 coaxial cable media with BNC connectors. Used by the LGS PC's.

10Base5: Also known as thick Ethernet; uses AUI drop cables (see below) to connect devices with a backbone cable.

10Base-T: 10 Mbps, uses Unshielded Twisted Pair (UTP) cable media with RJ45 connectors (telephone type).

100Base-T: 100 Mbps uses UTP Category-5 cable media with RJ45 connectors.

AUI -Attachment Unit Interface (drop cable) is used with 10Base5 (Thick) Ethernet and has DB15 connectors.

FDDI - Fiber-Optic Distributed Data Interface - a shared media LAN technology where all devices are connected in a ring using fiber optics. Devices share the common fiber "channel" by passing an electronic "token" (special sequence of bits) to indicate to each other who has permission to use the channel at a given time. Dual-attach FDDI implies two such channels, one transmitting clockwise around the ring and the other transmitting counter-clockwise. Optical bypasses are used on the SGI computers used by Landsat 7 to continue the connection in the event of a power failure on a particular machine so that the ring to other computers will not be broken. The 4 out of 5 encoding scheme is extremely efficient and real data throughput rates of 80 Mbps are achievable on nominally loaded networks.

1.6 Applicable Documents

The following documents contributed to the definition of the Landsat 7 Network Design:

NASA GSFC, 560-1ICD/0794, Interface Control Document (ICD) Between the Landsat 7 Ground Station (LGS) and the Landsat 7 Processing System (LPS) Revision 2, July 7, 1997.

NASA GSFC, 514-1ICD/0195, Interface Control Document (ICD) Between the Image Assessment System (IAS) and the Landsat 7 Processing System (LPS), Revision 2, January 26, 1998.

NASA GSFC, 511-4ICD/0296, Interface Control Document (ICD) Between the Landsat 7 Mission Operations Center (MOC) and the Landsat 7 Ground Station (LGS), Revision 2, October 1997.

NASA GSFC, LPS-104, Memorandum of Understanding Between the Landsat 7 Processing System (LPS) and the Landsat 7 Mission Operations Center (MOC), June 1997.

NASA GSFC, 511-4ICD/0197, Landsat 7 Mission Operations Center (MOC) to Landsat 7 Image Assessment System (IAS Interface Control Document (ICD), October 1997.

HITS, 505-41-32, Interface Control Document Between EOSDIS Core System (ECS) and the Landsat 7 System, Revision D, December 9, 1999.

NASA GSFC, 541-107 (CSC/SD-90/6509), NASA Communications (NISN) Access Protection Policy and Guidelines, Revision 3, November 1995.

1.7 Assumptions

The following assumptions were made in developing the Landsat 7 Network design:

1. Internet is sufficiently robust to handle traffic from GSFC to EDC even if that traffic must be sent daily.
2. NISN will provide IP addresses for all computers which interface with EBnet.
3. Network development does not include multiple paths for network traffic.
4. One of the key rules in network development is to separate the Operations side from the development side. There are numerous reasons for doing this including: configuration management, security, performance and interference. However, this separation was ground-ruled out from the start due to budget constraints on the LPS side (With only 5 Challenge XLs, the separation would have cost us the back-up string capability).
5. The EBnet router will provide connectivity from the LPS to the EDC DAAC as well as to EDC and other DAACs.

Section 2 - The EDC Network

2.1 Equipment

The EDC network is composed of a wide variety of devices of varying manufacturers and models. This is primarily due to the wide variety of projects and systems hosted by EDC. Recently, however, EDC has begun a concerted effort to standardize the network configuration, i.e., determine the best network equipment for all the systems at EDC and purchase only that type of equipment. Due to the philosophy followed at EDC routers for control, (star-type network) and requirements forced by the users (expandability, flexibility and performance), EDC has settled on 3-Com network equipment as our primary system.

2.2 Protocols

There are a number of routing protocols. Some of these protocols are standard, others are proprietary. In order to insure compatibility across the spectrum of system vendors, it is necessary that routers be capable of interpreting, understanding, and forwarding the most common protocols. In order to meet this requirement, router vendors implement software (such as 3Com's 'Complete Protocol Suite' for the NetBuilderII) which allows the network manager the option of routing, bridging, forwarding, or discarding input data packets. Although any given site will probably use only a few of the supported protocols, the large number of possible protocols greatly enhances the flexibility of the LAN.

The main protocols currently in use at the EROS Data Center are; Internet Protocol (IP), Address Resolution Protocol (ARP), Routing Information Protocol (RIP), Transmission Control Protocol (TCP), and Border Gateway Protocol (BGP). These protocols are used to encapsulate, transmit, control, and route data. In addition, Simple Network Management Protocol (SNMP) is supported and used to monitor and manage network resources.

2.2 EDC Supported Software

EDC supports a wide variety of software packages including: Microsoft Office, Word Perfect, and Novell Group-wise and numerous Unix tools. Software assistance tools such as IDL, Software Thru Pictures and eventually CASE are also available through the Site network. The functions provided by these packages are expected to be available to each resident at the EDC facility.

The IAS development being conducted at EDC requires the use of Software Through Pictures (StP). This tool will not be required after delivery of IAS to EDC.

Also, since the software programmers are located in a different place than the Landsat 7 system (due to EDC's matrix management system), the programmers will need network access to Landsat 7 systems at times. Some of these programmers divide their time between projects. These considerations are being answered with EDC office equipment at this time. PCs will be placed in the Operations Room for general use by any Operational personnel.

Section 3 - The Landsat 7 Network

3.1 Landsat 7 Network Design History and Future Plans

The Landsat 7 Network Design began with the developments in 1994. In October of 1996, EDC needed further definition of the network to order hardware to support the network at Sioux Falls. In October of 1996, EDC began discussing with NISN the Security Audit implications of the network connections to EBnet. Based on those discussions, EDC acquired copies of the NISN Access Protection Policy and Guidelines (See document list) and the with it the Security Audit checklist.

A meeting was held at GSFC on November 4 with EDC Ground System Integration Project Team, EDC Network Group (via teleconn), NISN, ECS and the EDC DAAC to discuss the NISN requirements, security audit and EDC's Site Preparation Plan. At this meeting the ground-rules for the self-certification were laid down and EDC Ground System Integration Project Team took an action to perform the self-certification of the EDC network.

A meeting was held at EDC on November 15 with EDC Ground System Integration Project Team, EDC Network Group, NISN (EBnet) and the element managers to discuss the timing and process for EBnet installation at EDC. At this meeting the self-certification for ECS was mentioned as underway.

On December 9 the group met again at GSFC to discuss the preliminary security audit checklist (provided by EDC Ground System Integration Project Team). At this time NISN Security was present and had numerous comments and suggestions. EDC took the action to incorporate those suggestions where possible and provide the completed checklist to NISN Security.

On March 10 of 1997, the completed checklist (Appendix A) was given to Jerry Knoll (CSC) representing NISN Security.

On March 14th of 1997, the AT&T service was provided to EDC. On March 18th, the routers were installed in computer room 3. In June, the LGS was hooked up to the Closed Segment of the MODnet.

In early-August, the LPS will be installed and hooked up to the EBnet routers. The IAS is scheduled to be connected to the Landsat 7 router in October and shortly after that, December 3rd, the final letter for the Security Audit will be sent from the security people at CSC to NISN. This will mark the end of the NISN network security audit, however, re-certifications are expected every three years afterwards.

3.2 Security Implications

Each element initially created their own internal networks independently. These networks were combined by EDC into a complete, workable system. EDC (specifically the Network Group) used the minimum cost approach to meet requirements.

Several system requirement changes have occurred since the initial design. One of the major changes in this network occurred as a result of the decision to implement S-band commanding and telemetry from the EDC. Command and telemetry have different security requirements than processing of down-linked data (X-band). A hacker who can get into the command and control section could conceivably sabotage the spacecraft. Therefore, the LGS was

put on the closed segment of MODnet to eliminate any path of security vulnerability. Since the LPS relies on the LGS for the Contact Schedule and Timing Data, the network was redesigned around an LPS connection to the MOC via Internet. A separate Network Time Protocol (NTP) Server was provided by EDC for the LPS.

Further changes resulted from security requirements imposed by NISN. These were primarily policy and protection system changes; however, it was decided to protect the "front-door" to Landsat 7 with a router based on NISN and EDC security considerations. On 2/2/9,2000 IAS machines were moved outside of the DHF router, but are secured via use of Secure Shell and disabling of the default route. The DHF router has a path open between LPS005 and IAS002/IAS001 for the CPF transfer.

3.3 Data Transfer Requirements

The chart below shows the files/connections required for Landsat 7 Operation:

Required Connections

From:/To:	LPS	LGS	IAS	MOC	EDC DAAC	Science
LPS				QR, Cap	L0R	
LGS				ESR,CSR		
IAS	CP			CP,CR,RCE	CP, RD, Reports	
MOC	CS	CS,SAD	NF,DE,TT		EEF,ESC	Ephemeris
DAAC	Req.		L0RS, SD			L0RS
Science			Algorithms			
NRL			Time Data			

Legend:

Cap	- Capture Summary	ESC	- Event Schedule
CP	- Calibration Parameter file	ESR	- Equipment Status Report
CR	- Calibration Scene Requests	NF	- Ascending/Descending Node files
CS	- Contact Schedule	QR	- Return Link Quality Report
CSR	- Contact Status Report	RCE	- Request for Concentrated Ephemeris
DAK	- Data Acknowledgement	RD	- Requests for Landsat 7 Data
DAN	- Data Availability Notification	Req.	- Requests for Reprocessing
DE	- Definitive Ephemeris	SAD	- Station Acquisition Data
EEF	- ETM+ Engineering File	SD	- Statistics Data
ES	- Event Schedule Report	SSR	- Spacecraft Status Report
		TT	- TLM Trending Analysis Report

The chart below shows anticipated usage of those connections:

Load Estimates

From:/To:	LPS	LGS	IAS	MOC	DAAC	Science
LPS				Neg	25GB/day	
LGS				Neg.		
IAS	Neg.			Neg.	Neg.	Neg.
MOC	Neg.	Neg.	Neg.		Neg.	Neg.
DAAC	Neg.		5 GB/day		1GB/day	
Science			Neg.			
Users					Neg.	

Neg. means negligible: either small files or large files transmitted infrequently.

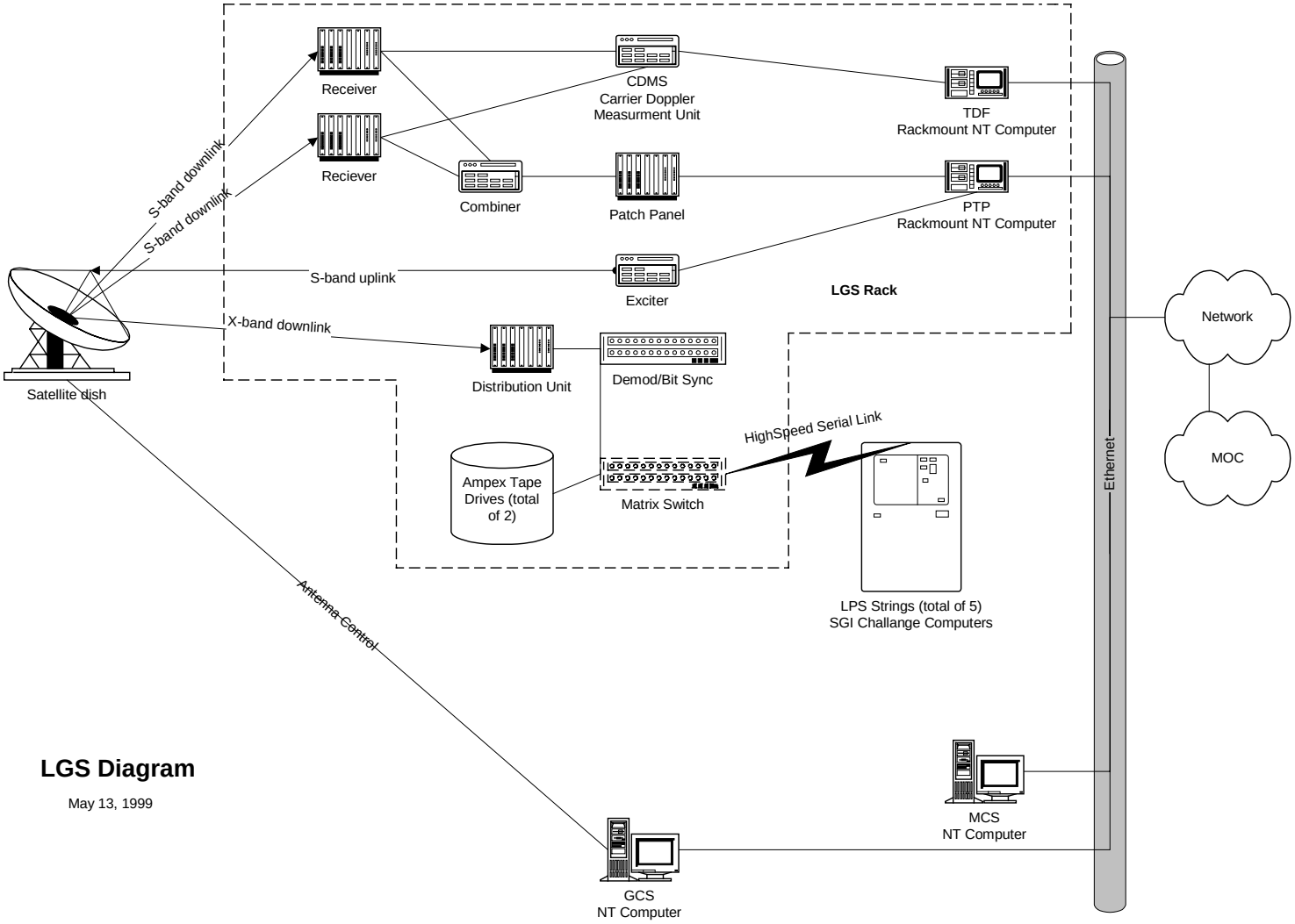
3.4 Hardware

The network hardware consists of the EBnet connections (a primary Cisco 7513 router and a backup Cisco 4700 router), the MODnet connections (two Cisco 2516 routers) and the EDC router (3-com Netbuilder II). The EBnet routers will be supplied by, installed by and maintained by NISN. The MODnet routers will also be supplied by, installed by and maintained by NISN. The EDC Exchange LAN router will be supplied by, installed by and maintained by EDC, however, several cards will be supplied by the Landsat 7 developer to support Landsat 7 functions. These routers are all located in computer room 3. See Appendix C for Specification sheets on these routers.

Four PCs are utilized by the LGS. These are the Monitor and Control System (MCS), the Ground Station Controller (GSC), the Programmable Telemetry Processor (PTP) and the Tracking Data Formatter (TDF). These four PCs are connected via dual -2516 router to the closed segment portion of the MODNET. All four of the LGS PCs use 10Base2 Ethernet. NISN will supply the connection needed to convert to 10 Base T required by the routers. The diagram shown in Figure 3.4.1 is shows the LGS hardware diagram.

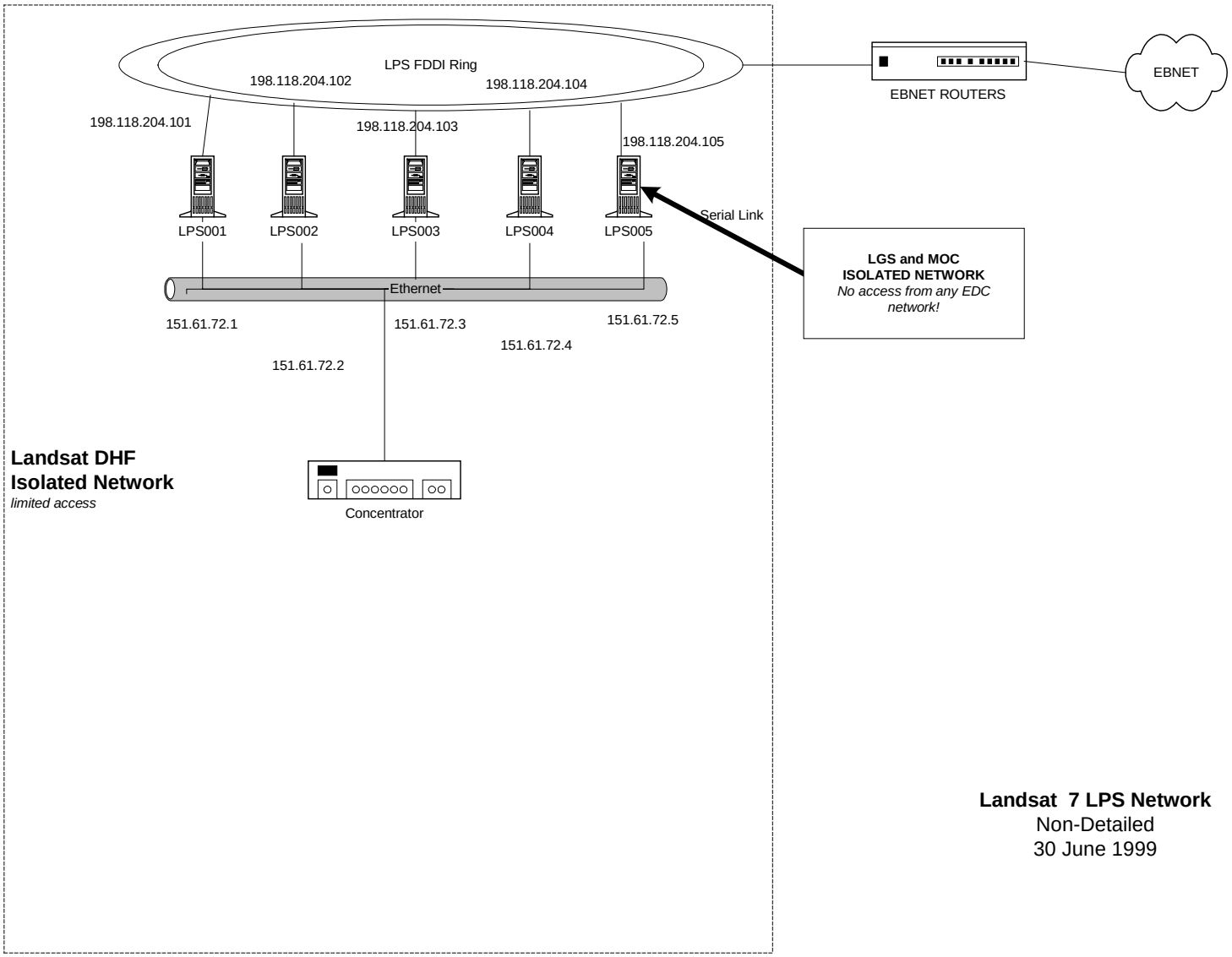
Five SGI Challenge XLs comprise the processing arm of LPS (R440 - 250MHz clocks). This side of LPS is connected to the EBnet router via dual-attached FDDI ring. Specification sheets on the Silicon Graphics computers are included as Appendix D.

Three SGI Indy workstations and 2 NCD X-terms comprise the workstation/displays. A 24-port Lancast hub connects these workstations with the Challenge XL's and the LPS printers. The hardware diagram is shown in Figure 3.4.2.



LGS Diagram

May 13, 1999

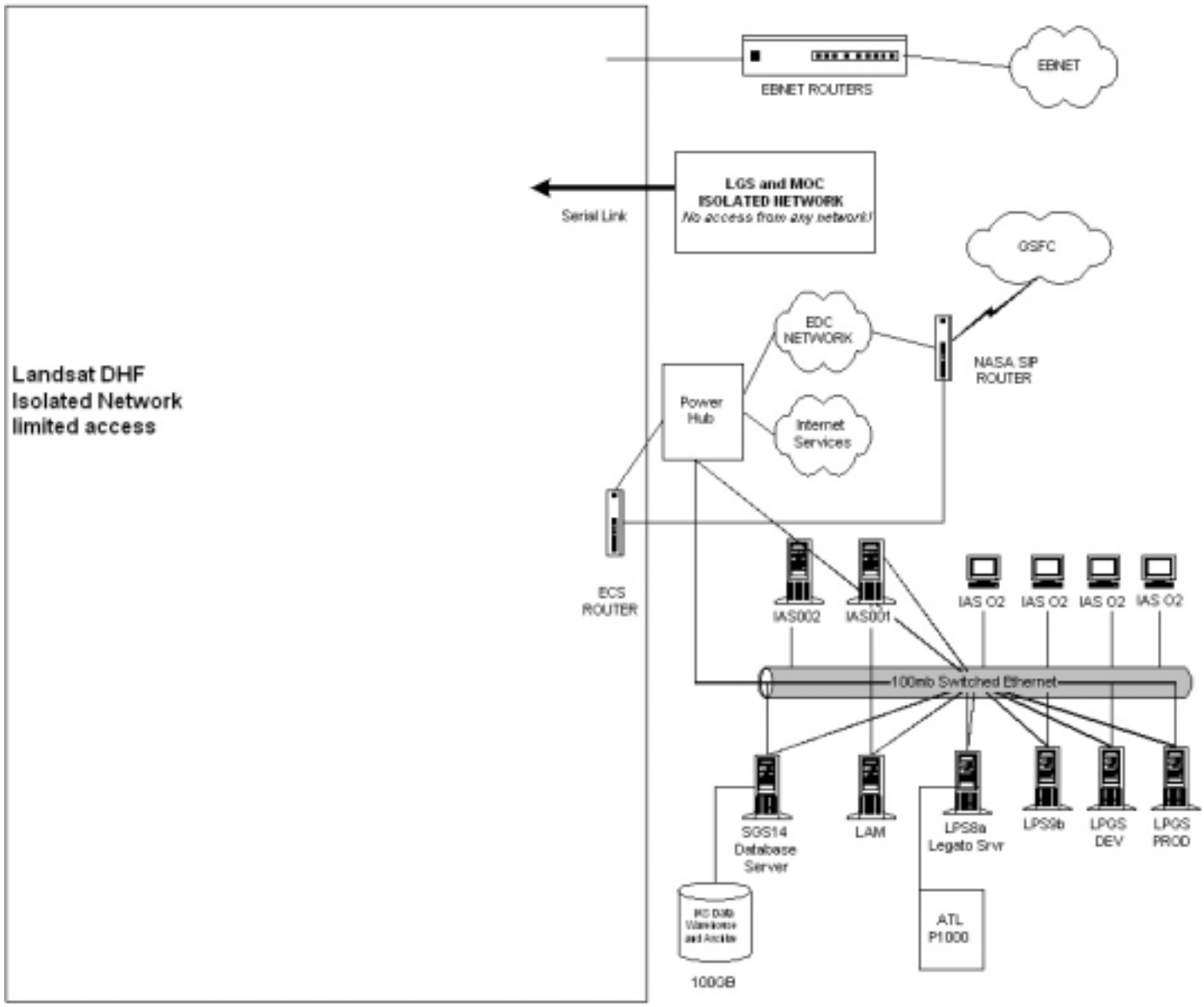


Landsat 7 LPS Network
Non-Detailed
30 June 1999

In order to support the transfer of scientific data to the IAS, three servers and two analyst workstations are connected to the EDC Exchange LAN router via 10/100 Fast Ethernet. This allows the required data transfer rate from the EDC DAAC. IAS hardware is shown in Figure 5.

IAS has requested the capability to upgrade to 100 Mbps. This was brought on by the Origin computers' capabilities. No hardware purchases to date, except the Origins, would support the 100 Mbps system, but this enhancement is not specifically ruled out by the current hardware design either.

Landsat 7 Network
Updated 2/25/2000



3.5.1 Security Software

In the course of the self-certification of EDC, several security packages were mentioned such as CRACK, SATAN, TCP Wrappers, and Tripwire. EDC is looking at each of these packages.

Tripwire is an integrity-monitor for Unix systems. It uses several checksum/signature routines to detect changes to files, as well as monitoring selected items of system-maintained information. The system also monitors for changes in permissions, links, and sizes of files and directories. It can be made to detect additions or deletions of files from watched directories.

The configuration of Tripwire is such that the system/security administrator can easily specify files and directories to be monitored or to be excluded from monitoring, and to specify files which are allowed limited changes without generating a warning. Tripwire can also be configured with customized signature routines for site-specific checks.

Tripwire, once installed on a clean system, can detect changes from intruder activity, unauthorized modification of files to introduce backdoor or logic-bomb code, (if any were to exist) virus activity in the Unix environment.

Further daemon logging is available via tcp_wrappers, which controls access to tftp, exec, ftp, rsh, telnet, rlogin, finger, and systat facilities. Its power is in its convenience: it can be installed without changing any system software components. Rather, /etc/inetd.conf is modified to invoke the tcpwrapper daemon before invoking any of its daemons. Tcp Wrapper then logs the connection and uses an access control list, if desired, to allow or disallow the access. The DHF is utilizing TCP Wrappers on its production machines.

3.5.2 Element Software - TBS.

3.5.3 Router Software - Cisco IOS.

3.6 Security Policy

3.6.1 EDC Security Policy

In November of 1996, EDC Security Policy was described as, numerous sections in several different documents in various people's control. These sections have been gathered together under one cover letter as Appendix B.

3.6.2 NISN policies

Refer to NASA Communications (NISN) Access Protection Policy and Guidelines (See document list).

3.7 Interfaces with other entities

Several organizations outside the EDC facility have requirements to communicate with the Landsat 7 DHF, the MOC, the Science Office/Team, for example. The DHF also has requirements to communicate with several organizations off-site as well, the Naval Research Laboratory, for one. These communication could be performed, although inadequately, using tapes, however, the preferred method would be via Internet. This method is not secure and further, it creates a security vulnerability, access to the DHF.

Appendix A - EDC Security Checklist

NASA Communications Access Control Compliance Checklist

Draft_v2
Date Completed

NOTE: ***The term "IT resources" refers to "data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data. This includes telecommunication systems, network systems, and human resources."***

A. CONFIGURATION

1. Name the Information Technology (IT) resource:
   Landsat 7 (L7) Data Handling Facility (DHF)

2. Provide the mission description of this IT resource.
   The Landsat 7 DHF process the data from the Landsat 7 spacecraft. This includes downlink, demodulation, preliminary data processing (Level 0R) and transfer to the storage entity, EDC-DAAC.

3. Provide a physical description of this IT resource. Attach legible block diagram(s) that identify PCs, workstations, servers, bridges, routers, gateways, firewalls, and external interfaces to the System, and connections to other networks. These diagrams should indicate the physical location of each major component of the system. Also, identify the network connections to this IT resource (e.g., NASA Internet (NI), center Local Area Networks (LANs), EBnet, NASA Communications 2000 Data Transmission, NOCS, IOnet Open Segment, IOnet Closed Segment). If firewalls on LANs and WANs are used, what components comprise the firewall design (Authentication Server, Screening Router, Bastion Host, Application Proxy Servers, other)?
   See attached.
   All devices comprising the DHF network reside at the EROS Data Center (EDC) in Computer Room #2, except the following. Access to these rooms are controlled by card-key locked doors. The EDC and ECS Networks are not confined to any of these described areas.

   L7 Ops Room
   L7Indy 3,7,8
   LPSx6, LPSx7
   L7NT_1
   L7o2_1
   hp1, hp2

   L7 Calibration Analysis Room
   L7ws004,5,6,7,8
   iaslj4
   (name) Rod Pater
   L7pc001,2,3
   IAS HP DesignJet
   HP JetDirect EX Print Server

   EDC Computer Room #3
   3Com Router (NetBuilder II)

4. Describe the security methods (both hardware and software) that are in place to protect this IT resource.
   Landsat Ground System (LGS) S/C Commanding – Connected to the NOLAN closed side of the router. LGS is also connected to LPS via a data link capable of bidirectional serial transmission. This link is only for data and clock, no protocol is involved. Flow is controlled by a matrix switch and a patch panel, neither of which can be remotely controlled.
   Software – Windows NT 4.0 (i386 HAL)

   LPS and IAS are connected to the EDC Campus LAN via the 3Com router. Access is by username and password.
   Software – Silicon Graphics variant of UNIX, IRIX.

   The 3Com router uses software enabling it to permit or deny access by IP address and service. This also permits or denies access based on which authorized host can initiate a connection.

   LPS is also hooked to the EBnet Router. IP address routing is denied by disabling the IRIX daemons routed and gated. On all machines where possible, kernel parameters enabling IP forwarding have also been disabled.

5. Identify which networks or systems (open and closed), this IT is connected to:

- Internet or NI? **Y/N:_N**
- Closed IOnet (including IPTX)? **Y/N:_Y**
- Open IOnet? **Y/N:_N**
- EBnet? **Y/N: _Y**
- Project procured carrier services? **Y/N:_N**
- Local LANs? **Y/N:_Y** via the 3Com router
- NISN ATM Network? **Y/N:_N**
- NREN? **Y/N:_N**
- AEROnet? **Y/N:_N**
- Other? **Identify:_____**

6. Is the software development system or test equipment for this IT capable of transmitting data directly or indirectly over NASA communications circuits or systems? **Y/N:_LPS005 is currently used for software development and as a "hot spare" to process L7 data. L7iasIT is used for integration and test of IAS software developed on L7iasDEV. L7iasDEV is located on the EDC Campus LAN. Software transfer is done via FTP through the 3Com router. This FTP connection can only be initiated from L7iasDEV. Connections allowed only when needed.**

7. Identify by title or position the individuals responsible for security of the IT resource, including the Network Administrators and CSO.

Individual	Title	Organization	Phone #
Ron Parsons	**CSB Chief**	**USGS/EROS Data Center**	**605.594.6555**

CSB: Computer Services Branch

B. INFORMATION TECHNOLOGY (IT) SECURITY CHECKLIST

1. ASSIGNMENT OF IT SECURITY RESPONSIBILITIES

1.a Has this project assigned a Computer Security Officer (CSO) in writing? **Y/N:_Y**

1.b Are IT security responsibilities included in the CSO's job description? **Y/N: _Y**

2. INFORMATION TECHNOLOGY SECURITY PLAN

2.a Is there a Security Plan(s) that covers all IT resources (government and contractor-operated)? **Y/N: _Y**
If yes, provide a copy of the Security Plan. **We will use USGS policies until local policies are approved. These policies, including the USGS Network Security Handbook, can be found at URL: http://www.usgs.gov:8888/ops/security/index.html**

2.b Has this plan been reviewed and updated within 3 years from its last update? **Y/N/NA: _Y**

3. AUTHORIZATION TO PROCESS

Has a Federal Management official authorized processing for each system, network and telecommunication system in the IT resource? **Y/N: _We are deciding who this should be.**
If yes, **Who: _____**

4. RISK MANAGEMENT

4.a Is there a Risk Management Plan(s) that covers all IT resources (government and contractor-operated)? **Y/N:_Risk Management Plan(s) will be developed by the end of the 1999 calendar year.**

4.b When was this plan last updated? **dd/mm/yy:_____**

4.c Was a Risk Assessment performed on the IT resources during the last two years? **Y/N:_N/A**

5. CONTINGENCY PLAN/DISASTER RECOVERY

5.a Has a contingency plan(s) that covers all IT resources (government and contractor operated) been prepared? **Y/N: _A contingency plan will be developed by the end of the 1999 calendar year.**

5.b When was the last time this project tested the contingency plan(s)? **dd/mm/yy:_____**

6. COMPUTER SECURITY AWARENESS TRAINING (CSAT)

6.a List all Computer Security Awareness Training (CSAT) conducted since the last GSFC Compliance Review.

TYPE	AUDIENCE	DATE
Computer Security	all EDC employees	(Yearly)

6.b Have any other CSAT activities been conducted? If yes, please list them.

TYPE	AUDIENCE	DATE

6.c Is security training provided whenever there is a significant change in the IT resources, environment or procedures? **Y/N:_N A formal plan will be developed by the end of the 1999 calendar year.**

6.d Did CSAT cover the following subjects? **See USGS Security Guidelines for the next items at URL: http://www.usgs.gov:8888/ops/computing/security/guidelines.html**

- Expected rules of behavior? **Y/N:_Y**
- Center Software Use Policy? **Y/N:_Y**
- Authorized use of government computers and computing resources? **Y/N:_Y**
- Incident handling? **Y/N:_Y**

7. INCIDENT REPORTING AND HANDLING

7.a List all IT security incidents that have occurred within the last six months. Include date of report and nature of incident.

Nature of the Incident	Date of report
None known on DHF network.	

7.b Has an incident response procedure been provided to each system and network administrator? **Y/N: _Y**

7.c Has the NASA Automated Security Incident Response Capability (NASIRC) contact information been provided to each system and network administrator? **Y/N: _Y**

8. LOGON BANNER

Has the NASA required logon banner been installed on each system? **Y/N: _**

UNIX machines yes, see the following. NT machines no. We are currently checking the possibility of adding this to our NT machines. Our NT machines are configured to refuse a telnet session.

<begin>

IRIX (l7iasit)

```
################################################################################
################################################################################
```

**** WARNING ***

YOU HAVE ACCESSED A U.S. GOVERNMENT COMPUTER. USE OF THIS COMPUTER WITHOUT AUTHORIZATION OR FOR PURPOSES FOR WHICH AUTHORIZATION HAS NOT BEEN EXTENDED IS A VIOLATION OF U.S. FEDERAL LAW AND CAN BE PUNISHED WITH FINES OR IMPRISONMENT (PUBLIC LAW 99-474). REPORT SUSPECTED VIOLATIONS TO THE SYSTEM SECURITY OFFICER. WHEN NECESSARY, CONTENT AND KEYSTROKE MONITORING IS UTILIZED TO PROTECT THE LOCAL AREA NETWORK FROM UNAUTHORIZED USE. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

```
################################################################################
################################################################################
```

<end>

9. NETWORK AND SYSTEM ACCESS CONTROL

Questions:	User Workstations	Admin Workstation **None**	Servers *	Routers *	Firewall * **None**	Test Equipment **
Number of individual users?	23 to 36 ***3**	**N/A**	38-70 ***3**	1 account.	**N/A**	***4**
Number of user groups?	16 to 20 ***3**	**N/A**	25-27 ***3**	**N/A**	**N/A**	**N/A**
Number of privileged users?	3 accounts, 2 of those are disabled.	**N/A**	3 accounts, 2 of those are disabled.	1	**N/A**	
Number of dial-in users?	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

Number of system administrators?	2, plus 1 hardware engineer with root password.	**N/A**	2, plus 1 hardware engineer with root password.	2 Network admin-istrators are assigned the task. The entire network group, 5 additional people, can be used when situations requiring backup personnel arise.	**N/A**	**N/A**
Are accounts disabled after a set number of failed logins?	No	**N/A**	No	No	**N/A**	**N/A**
If yes, what is the number?	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**
Does the system logoff or pause workstations and terminals automatically after 30 minutes of no keyboard and/or mouse activity?	Not without additional software.	**N/A**	Not without additional software.	Not without additional software.	**N/A**	**N/A**
Are requests for new users reviewed and approved by management?	Yes	**N/A**	Yes	Yes	**N/A**	Yes
Are users revalidated at least annually?	Yes	**N/A**	Yes	Yes	**N/A**	Yes
Are accounts promptly deleted when no longer needed or user changes job?	Yes	**N/A**	Yes	Yes	**N/A**	**N/A**
Are new users required to have security training prior to having an account?	Users attend security training within 90 days of hire.	**N/A**	Users attend security training within 90 days of hire.	Users attend security training within 90 days of hire.	**N/A**	Users attend security training within 90 days of hire.
Is a signed statement of responsibility kept on file for each user?	Yes	**N/A**	Yes	Yes	**N/A**	No

NOTES: * - in all cases these answers are for equipment under your organization's control. Do not attempt to answer for equipment that is controlled by another project or group such as NISN, EBnet or GSFC IOnet personnel.
** - Equipment such as network analyzers, sniffers, protocol analyzers, etc.

DHF notes: Many DHF servers and workstations can use the network interfaces in "promiscuous" mode for network troubleshooting. The software can only be used by priviledged users and is disabled by default.
***3 Accounts and groups include UNIX and NT overhead accounts such as root, lp, nobody, etc. Only user accounts are enabled for login.**
***4 The DHF network does not leave test equipment in operation when there is no need. The EDC network group keeps test and monitor equipment in their group office. That room is locked during non-work hours.**

10. PASSWORD MANAGEMENT

Questions:	User Work-stations	Admin Workstations **None**	Servers *	Routers *	Firewall * **None**	Test Equipment **
Are passwords required for all accounts?	Yes	**N/A**	Yes	Yes	**N/A**	**N/A**
Are group passwords used?	No	**N/A**	No	No	**N/A**	
Is password unique for each user except for operations?	No	**N/A**	No	**N/A**	**N/A**	
If not unique, how many people share the password?	Sys admins share root account password.	**N/A**	Sys admins share root account password.	Network admins share router password.	**N/A**	**N/A**
Is password unique for each operator?	Operators use "ops" account.	**N/A**	Operators use "ops" account.	**N/A**	**N/A**	**N/A**
Is Password unique for each device? ***5**	No, Same admin-istrators for these devices.	**N/A**	No, Same administrators for these devices.	No, Same admin-istrators for these devices.	**N/A**	**N/A**
Is password unique for each location?	1 location involved	**N/A**	1 location involved	1 location involved	**N/A**	**N/A**
Are one-time or safe passwords used?	No	**N/A**	No	No	**N/A**	**N/A**
Minimum password size?	6	**N/A**	6	6	**N/A**	**N/A**
Maximum password size?	8 UNIX 14 NT	**N/A**	8 UNIX 14 NT	>8	**N/A**	**N/A**
Both upper and lower case letters required?	No	**N/A**	No	No	**N/A**	**N/A**
At least one number required? ***6**	Yes	**N/A**	Yes	Yes	**N/A**	**N/A**
At least one special character required? ***6**	No	**N/A**	No	Yes	**N/A**	**N/A**
Is password composition checked?	Only by O/S software	**N/A**	Only by O/S software	No	**N/A**	**N/A**
Is password changed periodically? ***7**	Yes	**N/A**	Yes	Yes	**N/A**	**N/A**
What is the password change period?	Users 90d root 30d	**N/A**	Users 90d root 30d	90d	**N/A**	**N/A**
Is password change interval software enforced?	Users Yes root No	**N/A**	Users Yes root No	No	**N/A**	**N/A**
Are passwords automatically disabled 30 days or less after change period expires?	Passwords disabled at expiration date.	**N/A**	Passwords disabled at expiration date.	No	**N/A**	**N/A**
Do all superusers and system administrators have a regular login account (non-privileged)?	Yes	**N/A**	Yes	**N/A**	**N/A**	**N/A**

***5 The same administrators maintain their assigned equipment. "Root" passwords are the same on different machines. This reduces the possibility of written passwords being either posted in public places or lost.**

***6 At least on non-alpha character required by policy. OS only verifies numbers are included in password.**

***7 Some other situations where passwords are changed include. Root and/or operator passwords are changed when root or operator personnel changes. Users are alerted to change their passwords when network diagnostic/test equipment have recorded network traffic.**

11. CONFIGURATION MANAGEMENT (CM)

Questions:	Work-stations	Servers *	Routers *	Firewalls * **None**	Test Equipment**	Network Monitor * **None**
Is a CM process in place?	Yes	Yes	Yes	**N/A**	Yes	**N/A**
Do CM personnel approve Operating System (OS) file changes?	Yes	Yes	Yes for software or firmware changes.	**N/A**	Yes for software or firmware changes.	**N/A**
Do CM personnel maintain listings of approved software?	Yes	Yes	Yes	**N/A**	Yes	**N/A**
Do CM personnel retain records on at least current and previous configurations?	Yes	Yes	Yes	**N/A**	Yes	**N/A**
Do CM personnel document approved configuration changes?	Yes	Yes	Yes	**N/A**	Yes	**N/A**
Do CM personnel ensure only authorized software and configurations are installed?	Yes	Yes	Yes	**N/A**	Yes	**N/A**

12. SOFTWARE

Questions:	Workstations	Servers *	Routers *	Firewall * **None**	Test Equipment **
Is COTS software used?	Yes	Yes	Yes	**N/A**	Yes
Is public domain software used?	Yes	Yes	No	**N/A**	No
How often are backups performed (interval)?	TBD based on data requirements after launch.	TBD based on data requirements after launch. LPS strings 1-4 are considered backups of each other.	Before each firmware or software change.	**N/A**	**N/A**
Are backups stored off site?	No	No	No	**N/A**	**N/A**
How often are backups tested (interval)?	TBD based on data requirements after launch.	TBD based on data requirements after launch.	Testing backing would be disruptive to the network.	**N/A**	**N/A**
Are OS and security patches kept up to date?	Yes	Yes (OS patches only done if required.)	Revision releases are the only upgrades.	**N/A**	**N/A**
How long are backups retained?	TBD	TBD	At least one generation.	**N/A**	At least one generation.
Are only specifically needed server processes enabled?	Yes	Yes	**N/A**	**N/A**	**N/A**
Are there trust relationships between computers?	No	Yes. Controlled by /etc/host.equiv file between IAS002 and L7iasIT only.	**N/A**	**N/A**	**N/A**
Is exporting of whole file system allowed?	Yes ***8**	Yes ***8**	**N/A**	**N/A**	**N/A**
Can root be exported?	Yes ***8**	Yes ***8**	**N/A**	**N/A**	**N/A**
Is privileged software only able to be run from controlled sources?	***9**	***9**	**N/A**	**N/A**	Physical access is limited.

***8 Entire filesystems can be exported using NFS software. DHF has designed the directory structure so that if an entire filesystem is to be exported, that filesystem contains only relevant data. An NFS-export list, /etc/exports, is maintained so only approved hosts can mount the filesystems.**

***9 Access to DHF systems is controlled by networked machines located behind card-key locked doors or by the 3Com router denying all but specific EDC IP addressed machines network access. The 3Com router further limits those machines to only specific services and what hosts may initiate the connection. Routers on the EDC Campus LAN, external to the DHF network, are configured to detect and deny network access of machines external to the EDC Campus LAN *spoofing* EDC internal IP addresses.**

13. AUDIT TRAIL

Questions:	Workstations	Servers *	Routers *	Firewalls *	Test Equipment **	Network Monitor * **None**
Does equipment generate audit records?	Yes, UNIX syslogs.	Yes, UNIX syslogs.	No, diagnostic logs are kept.	**N/A**	**N/A**	**N/A**
Is access to audit records limited to authorized personnel only?	No	No	Yes	**N/A**	**N/A**	**N/A**
How often are audit records reviewed?	"Big Brother" software examines the syslog file for predetermined words and phrases every five minutes and displays an alert if necessary.	"Big Brother" software examines the syslog file for predetermined words and phrases every five minutes and displays an alert if necessary.	When there is a problem.	**N/A**	**N/A**	**N/A**
How long are audit records retained? (Time in days or months)	1 previous week	1 previous week	30d	**N/A**	**N/A**	**N/A**
Which of the following are logged:						
• System access/usage	Yes	Yes	**N/A**	**N/A**	**N/A**	**N/A**
• Logins/logouts	Yes	Yes	**N/A**	**N/A**	**N/A**	**N/A**
• Failed login attempts	Yes	Yes	**N/A**	**N/A**	**N/A**	**N/A**
• Break in attempts	Some	Some	**N/A**	**N/A**	**N/A**	**N/A**
• Unauthorized file access	Some	Some	**N/A**	**N/A**	**N/A**	**N/A**
• Privileged user actions	Yes, UNIX history facility.	Yes, UNIX history facility.	**N/A**	**N/A**	**N/A**	**N/A**
• Attempts or modifications to user authorization files	Yes	Yes	**N/A**	**N/A**	**N/A**	**N/A**
• Attempts or modifications to audit log	No	No	**N/A**	**N/A**	**N/A**	**N/A**
• Attempts or modifications to critical files	No	No	**N/A**	**N/A**	**N/A**	**N/A**
• Dial-in modem traffic	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

14. DIAL-IN/REMOTE ACCESS

14.a Is Dial-In access allowed? **Y/N: _N**

14.b Who authorizes this access? **Title:_____**

15. ENCRYPTION OF UNCLASSIFIED DATA

15.a Is encryption employed? **Y/N: _Other than account passwords, no.**
If yes,

15.b Has a key management process been established and maintained? **Y/N: _N/A**

15.c Has a data recovery process been established and maintained to ensure that NASA information is accessible? **Y/N: _ N/A**

15.d Has a process been established that encrypts passwords if it is possible for either privileged or non-privileged users to browse memory or disk storage where passwords are kept? **Y/N: _ N/A**

15.e Has a process been established that encrypts password files on backup tapes if it is possible for either privileged or non-privileged users to browse the tapes? **Y/N: _ N/A**

15.f Has a process been established that encrypts private data if the system has no other mechanism for providing controlled browse access protection to the data? **Y/N: _ N/A**

15.g Has a process been established that encrypts private files on backup tapes if the tape library system has no other mechanism for providing controlled browse access protection to the data? **Y/N: _ N/A**

15.h Is data encryption compliant with NIST standards used? **Y/N: _ N/A**

15.i Has the NASA Communications System Security Officer (SSO) approved the non-use of data encryption (or use of non-compliant encryption)? **Y/N/NA: __N/A**

16. SOFTWARE PROTECTION

16.a Has IT security established a policy to ensure compliance with the Center Software Use Policy? **Y/N: _Y We use the USGS policies in lieu of local policies.**

16.b Has anti-virus software been installed on all personal computers? **Y/N:_ Yes. Being installed now (3-25-99)**

16.c How frequently is the anti-virus software updated? **Monthly**

16.d Have IT personnel been briefed on the proper steps to take whenever they encounter a virus? **Y/N: _Yes, at CSAT briefing.**

16.e Have personnel been briefed of their responsibilities regarding the installation of licensed software on IT resources? **Y/N: _Yes, at CSAT briefing.**

17. SECURITY SOFTWARE

17.a Is there any security software (i.e., Vendor-provided or freeware software like SATAN, ISS, COPS, Crack. etc.) used to test the security vulnerabilities of this IT? **Y/N: _Currently no. this is in the initial stages of consideration.**

17.b If yes, **list:_____ N/A**

17.c If yes, have the identified security vulnerabilities been corrected? **Y/N: _ N/A**

18. PHYSICAL SECURITY

18.a What physical security barriers are in place (e.g., office doors locked when not occupied or after normal work hours)? **Explain: DHF equipment in card-key locked rooms. Building access controlled after normal work hours.**

18.b Do you train employees to challenge unknown personnel encountered in the work area? **Y/N: _Currently No. This policy will be added in any Risk Management Plan developed by the DHF staff.**

19. DESTRUCTION OF IT PRINTOUTS

19.a Does this IT resource handle "For Official Use Only," Procurement Sensitive, or proprietary information? **Y/N: _N**

19.b If so, how is this information destroyed? **Explain: N/A**

20. DISPOSAL OF IT RESOURCES HARDWARE /MEDIA

20.a Does the project have a procedure in place to ensure that any media containing sensitive data is sanitized before disposal? **Y/N: _N/A**

20.b Has the procedure been provided to users of IT resources? **Y/N: _ N/A**

21. MEDIA STORAGE

21.a Is the media protected from theft and vandalism? **Y/N: _Y**

21.b If using a storage facility, is the access restricted? **Y/N/NA:_Y**

21.c Is sensitive information identified with an external label? **Y/N: _N/A**

22. NETWORK SECURITY

22.a Are established protocols and network devices with proven error detection used? **Y/N: _Y**
22.b Is physical access to network components limited to authorized personnel? **Y/N: _Y**
22.c Is session termination information transmitted to the other partner when one session partner disconnects either normally or abnormally? **Y/N:_Y**
22.d Are there trust relationships between computers? **Y/N: _Y IAS002 and L7iasIT. Limited by /etc/hosts.equiv file.**
22.e Is file sharing limited to specific files and not the whole file system or partition? **Y/N: _N File sharing is limited to authorized hosts in /etc/hosts.equiv and authorized hosts and specific filesystems in /etc/exports.**
22.f Are configuration changes and console commands restricted to authorized personnel only? **Y/N: _Y**
22.g Are one-time passwords or authentication methods other than clear-test passwords used for remote login or remote control? **Y/N: _N**
22.h If yes, **Explain:**
22.i Are there any network nodes connected to both a protected network and a non-protected network? **Y/N: _Y The 3Com router**
22.j Are internal connections isolated from mission networks? **Y/N: _Y**
22.k Are there any indirect interfaces to NASA Communication? **Y/N:_N Describe.**
22.l Are there any restrictions on remote users? **Y/N: _Y**
22.m If yes, do these restrictions apply to system administrators and other users with root privileges? **Y/N: _Y**

23. IONET CONNECTIVITY

23.a Are there connections to any other network for those IT resources that connect to the Closed IOnet? **Y/N:_Yes. Describe.** The LPS and LGS are connected via a data line capable of carrying bidirectional, serial data. The LGS controls the direction, source and destination of the data flow. Typically, the LPS receives data from either the antenna or Ampex tape or the LPS plays previously recorded data to the Ampex tape drives located in the LGS racks for shipment to other stations. The serial data stream transmitted over the data line contains no protocol, only data and clock signals.
23.b Is a router used between connections on the Open IOnet and other networks? **Y/N: _N**
23.c Are all connections between the Open and Closed IOnet made via the Goddard Secure Gateway? **Y/N:_N/A**

24. FIREWALLS

24.a Are local firewalls used? **Y/N: _No**
If yes,
24.b Is all firewall administration performed from the local terminal or via a Virtual Private Network? **Y/N: _ N/A**
24.c Are accounts on the firewall limited to system administrators? **Y/N: _ N/A**
24.d Are firewall logs examined at least weekly? **Y/N: _ N/A**
24.e Is the firewall run on a dedicated computer? **Y/N: _ N/A**
24.f Are IT services to the general public kept outside the firewall? **Y/N: _ N/A**
24.g Are deny-based rules used for connections originating outside the firewall to systems inside the firewall? **Y/N: _ N/A**
24.h Are allow-based rules used for connections originating inside the firewall to outside the firewall? **Y/N: _ N/A**
24.i Are connections between systems inside and outside the firewall passing through the firewall for authorization, logging, and monitoring? **Y/N: _ N/A**
24.j Is OS and firewall software kept-up-to-date? **Y/N: _ N/A**
24.k Does the firewall limit the services allowed through the firewall? **Y/N: _ N/A**

Appendix B - EDC Security Policy

COMPUTER AND NETWORK SECURITY HANDBOOK

U.S. GEOLOGICAL SURVEY

TABLE OF CONTENTS

11.4 Incident Reporting

SECTION 1. INTRODUCTION

The Computer Security Act of 1987, Public Law 100-235, established the framework for Federal agencies to improve the security and privacy of sensitive information in their computer systems. To comply, the U. S. Geological Survey (USGS) has established a comprehensive information systems security program. The development and distribution of computer security policy and guidelines are major components of this program.

The main objectives of this document, The USGS Computer and Network Security Handbook, are to extend the policies set forth in the Survey Manual's Chapter 600.5 on Information Systems Security and to provide USGS employees and contractors with a ready reference for implementing distributed processing security controls. This document addresses a broad set of information systems security control techniques including those of:

* System, physical, software, and data protection;

* Personnel and administrative procedures;

* Risk management and contingency planning; and

* Computer security plans and reviews.

USGS senior management officials encourage the use of this handbook as one of several tools for managing, controlling, maintaining, and implementing an effective Information Technology Security Program for the bureau. This handbook should not be considered a static document. Changes in technology, the hazards which threaten resources, and the manner in which business is conducted, will impact the USGS's network environments and the USGS's Information Technology Security Program. Additional guidelines and revisions to this handbook will be generated as needed.

With the advent of Local Area Network (LAN) and Wide Area Network (WAN) systems which distribute functions and data away from centralized mainframe computer centers, there comes the responsibility for applying information systems security concerns which were primarily in the realm of centralized data processing. Few organizations have been immune to the general trend toward downsizing systems from mainframes to LAN and WAN based architectures and the USGS is no exception.

The USGS's networked systems consist of thousands of personal computers, UNIX and NT workstations, mainframe, dial-in facilities, and a variety of servers linked together using numerous technologies. These networks provide connectivity to all USGS sites to facilitate the processing of scientific and administrative information.

Sensitive information resides on and passes through most components of the Survey's networks. Therefore, it is important that appropriate safeguards

be implemented at those points where sensitive information is created, processed, or stored. As information resources functions are distributed so are the responsibilities for safeguarding hardware, software, communications, and data. USGS's senior management officials recognize the importance of protection in distributed processing environments. Although a totally secure system is unobtainable, the procedures and guidelines offered here are aimed at reducing the risks associated with inadequately protected networks by providing an appropriate level of security which is consistent with risks involved and within the constraints imposed by USGS data and information resources.

1.1 GOALS AND OBJECTIVES

The primary goals and objectives of any effective computer security program are:

* Confidentiality - Ensuring that USGS sensitive data, sensitive information, and sensitive systems are kept private and are accessible only by authorized personnel on a need-to-know basis;

* Integrity - Ensuring that all USGS data and information are accurate, timely, and complete; and

* Availability - Ensuring that all USGS data, information, and systems are ready for use when they are needed.

1.2 HOW TO USE THE HANDBOOK

This handbook is intended to be used as a supplement to the USGS's information systems security policy and defines an additional set of security controls that are intended to meet or exceed the general requirements previously established by the Department of the Interior, Office of Management and Budget, General Services Administration, National Institute of Standards and Technology, and the Computer Security Act of 1987.

All USGS employees and contractors should read the following information systems security documents:

* Survey Manual Chapter 600.5 Information Systems Security: General Requirements;
* DOI Manual 375 DM 19; and
* DOI Automated Information Systems Security Handbook. (contact the BITSA for copies)

These documents provide general information and requirements regarding the Department's and USGS's Information Technology Security Program. For additional material on computer security in the Federal sector, refer to the security web site at: http://www.usgs.gov:8888/ops/computing/security/

The USGS Information Technology Security Program is built on the premise

that all USGS system users play a major role in safeguarding and protecting all of the bureau's information assets.

Note: The policies and guidance provided in this document will almost definitely be superseded by new ones. What seems important or adequate today may not be tomorrow. We should be prepared to continually review and change, when necessary, our computer security requirements and policies to meet changing technologies, the needs of our users, the changing threat environment and future Federal computer security regulations.

SECTION 2. WORKSTATION AND NETWORK COMPONENTS

2.1 WORKSTATIONS

For the purpose of this handbook, a workstation is defined as any intelligent terminal device, single (PC or MacIntosh-based) or multi-user (UNIX, Linux, or NT) processor that may or may not be connected to networks. Although portions of this document are applicable to standalone workstations, the focus is on networked workstations.

2.2 NETWORK COMPONENTS - GENERAL

Network infrastructures (LAN's, Intranets, etc.) tend to be complex and their configurations must be defined before certain security requirements can be determined and responsibilities assigned. The definition of a network component can be based on one or more of the following three criteria: physical (campus, building, floor, etc. boundaries); organizational (bureau, division, office, etc.); or functional (finance, geologic mapping, general administration, etc.).

In environments such as the USGS headquarters building where much of the network infrastructure is shared, organizations must work cooperatively to determine the most appropriate network component structure. In fact certain aspects of the network such as the backbone, may be managed independently from those components that are owned by the divisions.

It is the responsibility of management to ensure that all network components are adequately defined so that all the parts of the network infrastructure are covered. This is required to help guarantee that the responsibility for security is assigned and appropriate security controls are in place and effective for each network component.

* For the purposes of this document and the policies contained within, the USGS Intranet is defined as those devices located within the network domains of usgs.gov.

2.2.1 NETWORK COMPONENTS - HARDWARE

A LAN consists of a number of workstations connected via cabling to a server and/or shared services such as networked printers, scanners, or FAX machines. It generally is confined to a single building or even one floor

of a building but could extend to multiple buildings in a geographically confined space. LANs generally utilize client-server architecture and are configured so as to split the processing of an application between different components. That is:

* A client component, a personal workstation with a full range of features for running applications; and

* A server component that may be another personal computer, a minicomputer, or a mainframe, which provides data management and information sharing available for use among multiple clients.

LANs may also provide access to the USGS mainframe computer system which is located at the National Center, Reston, VA. USGS LANs are typically connected to the Department Of Interior Network (DOINET) which is a WAN that links DOI field offices or the Internet. This is accomplished via networking devices such as repeaters, bridges, routers, and gateways. The type of device which is used depends on a complex set of communications protocols, or rules, that computers use to control the flow of messages between them.

LAN cabling physically connects the components of the LAN. Cabling may take the form of "twisted-pair" cable, coaxial cable, or optical fiber. Some LAN's are connected by a combination of these.

Servers are generally dedicated computers that provide various types of support to the client workstations such as application functions, file storage, and communication handling. Network management systems are installed on LAN servers to manage network access and communications, resources allocation and sharing, data protection, and error control. The network management systems also monitor network traffic and store network information for subsequent analysis.

2.2.2 NETWORK COMPONENTS - APPLICATIONS

Network applications are normally of a type that include distributed file storage, messaging, and remote computing. A LAN connects servers, workstations, mass storage devices and printers through one or more common network operating systems which enable users to share the resources of the LAN.

More specifically, distributed file storage allows users to access, retrieve and store files by providing an attachment to a remote mass storage device called a file server. To the user, it appears as if the disk drive is a local workstation drive thus the function is basically transparent to the user. Remote printing is also considered as a distributed file storage type of function. A user may print to any printer on the LAN which is attached to one of the LAN workstations. Consequently, expensive printers can be shared and LAN print servers can accept print files freeing up local workstations so that work can be continued instead of waiting for print jobs to complete.

Remote computing refers to users remotely logging in to another component on the LAN, executing an application that resides on another component, or running applications on other components while appearing as if they were running on the local work station.

Messaging applications relate to electronic mail and conferencing. Mail servers provide the capability to send and receive messages across a LAN like a private mail service.

USGS systems consist of standard office automation packages for word processing, calendaring, and electronic mail. Additionally, UNIX-based servers run relational database management systems such as Oracle. Other UNIX-based servers act as electronic mail gateways allowing electronic mail exchange between USGS sites.

SECTION 3. SECURITY CONTROL ENVIRONMENT

Information system safeguards must be made more robust to challenge the added threats associated with transmission of data and commands over communication lines which may be open to public use. Consider that processing functions in a distributed environment may pass through several "services" prior to the requested action being completed. A requested action may pass from a workstation (microcomputer) over communication lines to a LAN server. The server may be attached to a bridge or gateway which directs the message over additional communication lines (which may be private or public) into another LAN. Once there, the message may go to another server for data or to another workstation. The demand for protecting sensitive information is actually increased by the fact that the majority of processing is LAN-based. Each "service" must provide the security safeguards which will protect the confidentiality, integrity, and availability of the information and systems.

3.1 WORKSTATION AND NETWORK SECURITY THREATS

There are many information systems security threats which can potentially violate the security networked environments. These threats could originate from intruders (hackers), malicious computer code (viruses, Trojan horses)), defective equipment, manmade or natural hazards, and even authorized users.

Threats can normally be categorized into having one of the following effects:

* Compromise;

* Loss of Integrity; and

* Denial of Service.

3.1.1 COMPROMISE

Compromise is the unauthorized disclosure of sensitive information. Networks where every node can access all of the data in the environments are most vulnerable. As a user on the LAN, it is easy to install network analysis software on any connected computer and read all of the traffic traversing the LAN or WAN.

Unauthorized disclosure may also occur when an individual who is not entitled to the data gains access and releases it.

Compromise is possible when:

* Unauthorized access occurs due to access privileges which are too permissive or access control mechanisms which are improperly or poorly implemented;

* Workstations are left unattended and\or unprotected while logged on to a networked application;

* User authentication and/or data are transmitted in clear text form over the network;

* Application source code is not adequately protected;

* Network monitoring devices or software are not properly controlled;

* Printers that handle sensitive data are located in high traffic, uncontrolled areas; and

* Data backup copies are not stored in secure areas.

3.1.2 LOSS OF INTEGRITY

When a system is exposed to accidental or intentional malicious alteration or destruction there is a loss of integrity. In networked environments, this may occur by:

* Data modification when nodes of the network can modify frames sent on the network and then retransmit the modified versions;

* The replaying, or repeating, of a message to produce an unauthorized result such as copying a message destined for a different node and then replaying it later;

* Execution of malicious code;

* One entity masquerading, or pretending, to be another entity and accessing unauthorized messages; and

* Unauthorized use of a resource because authorized nodes are trusted and have unchallenged access to other data resources on the network.

3.1.3 DENIAL OF SERVICE

When an authorized entity cannot gain access to network resources, or when time critical operations are delayed, it is a denial of service. Denial of service can result from:

* Physical damage to workstations or network components (like a cut cable) or power outage;

* Flooding or jamming the network by continuously transmitting messages;

* Lack of an adequate continuity of operations plan; and

* Infection of networked devices by malicious code.

3.2 LAYERS OF PROTECTION

Controls for protecting USGS data and information resources against network security threats are applied in layers. The controls may be manual or automated with the outer-most layers providing less protection than the more complex inner layers.

The security layers include:

* Management or Procedural Controls - The numerous administrative controls that exist around any system including personnel procedures, security and awareness training, security standards, and procedures for system development, testing, documenting, and operation;

* Physical Controls - The controls used to limit a person's physical access to system components, as well as building security, control over the environment, and protection for the physical being of people and equipment;

* Access Controls - The software and hardware which limits access to computing resources; and

* Telecommunications Controls - The controls, normally included in vendor's communication products, for identifying messages with users, routing messages, and controlling the flow of data between network nodes.

* Data Integrity Controls - The controls assuring that data is protected from unauthorized change during storage or transmission.

Some or all of the control layers will be applied for protecting USGS network environments and component services.

SECTION 4. WORKSTATION AND NETWORK SECURITY MANAGEMENT

The USGS Information Technology Security Program is impacted by everyone having authorized access to USGS data and information resources. Consequently, all USGS system users have roles and responsibilities within the program. Since USGS's Information Technology Security Program is a major on-going and evolving effort, so are the associated roles and responsibilities. The management and ethical operations of USGS network environments involve specific support roles with associated responsibilities.

It is important to recognize that duties must be performed associated with these roles. The assignment of these responsibilities will include specific management and technical training, the appropriate separation of duties, and designating employees at a level in the organization with specific responsibilities and accountability. In smaller organizational units, the line manager and network administrator may actually be the same person. In these instances, responsibilities may be combined or shared.

This section details specific components of the USGS Information Technology Security Program and the requirements for implementing and operating an effective workstation and network computer security program.

4.1 RESPONSIBILITIES

The USGS's Information Technology Security Program is managed by the Bureau Information Technology Security Administrator (BITSA). The BITSA responsibilities include:

* Managing, implementing, and enforcing an effective and sound Information Technology Security Program for the USGS in accordance with USGS, DOI, and Federal laws, policies, directives, standards, and guidelines;

* Establishing policies, standards and guidelines for controlling access to USGS networks and systems;

* Conducting periodic computer security reviews of USGS workstation and network environments, reporting control weaknesses, and recommending additional security measures;

* Ensuring that an effective security awareness training program is in place to educate all managers, users, IT officials on the importance of maintaining and safeguarding all USGS systems and information; and

* Communicating all computer security incidents in writing to appropriate officials with recommendations for immediate and future corrective actions.

USGS Line Managers and Supervisors are responsible for:

* Implementing established computer security policies within their areas of responsibility including the prescribed Rules of Behavior (See

Section 4.4);

* Promoting computer security awareness and ensuring employees are knowledgeable of their responsibilities associated with the use of USGS computing resources and of the possible ramifications if misused;

* Ensuring computer security requirements are included in specifications and contract documents for acquisition or operation of computer facilities, equipment, software packages, or related computer services;

* Ensuring that all breaches of computer security, events that may indicate a computer security incident or violation, or attempts to gain unauthorized access to computers, information systems, or data resident on USGS information resources are reported.

* Ensuring that User IDs for employees or contractors who are terminated are deleted and data sets assigned to those IDs are reassigned to another authorized user in the organization.

The Network Administrators are responsible for:

* Serving as the primary point of contact for network computer security and access control;

* Administering and coordinating network access authorization process and procedures;

* Implementing all appropriate network security policies, standards, rules, and procedures;

* Monitoring network activities;

* Assisting in periodic computer security reviews of network components to ensure adequacy of security measures and safeguards;

* Reporting all violations of computer security incidents to immediate supervisor and the BITSA;

* Performing daily backup and recovery procedures on local file servers; and

* Refraining from exploiting system privileges such as intentionally modifying, destroying, reading, or transferring data and information in an unauthorized manner.

The workstation and network users are responsible for:

* Obtaining required computer security awareness training and abiding by all USGS Rules of Behavior (see Section 4.4);

* Following appropriate procedures for requesting permission to access network resources;

* Selecting unguessable passwords;

* Ensuring that passwords are held in strict confidence and properly safeguarded from unauthorized access and unauthorized use;

* Following and adhering to USGS computer and information systems security policies, standards, procedures, and guidelines to safeguard and protect all USGS data and applications, including the utilization of file protection mechanisms to maintain appropriate file access control;

* Ensuring that regular backups are made of all critical data stored on their own workstation(s) and ensuring that sensitive data is deleted from the hard drive(s) prior to disposal of the machine;

* Obtaining supervisory approval prior to introducing any non-government purchased software including freeware into USGS computing environments;

* Ensuring that all software and documents are scanned for viruses prior to loading onto those USGS workstations or network devices that are susceptible to viruses;

* Controlling file and share-level access to resources when operating in a peer-to-peer environment;

* Reporting any observed or suspected computer security incident or violation to your immediate supervisor, network administrator, or the BITSA;

* Requesting that their accesses to all USGS systems are deleted or suspended prior to leaving the employment of the USGS and that all critical data sets identified with their User ID's are transferred to another, authorized employee; and

* Ensuring that terminal sessions (Windows, etc.) are rendered unaccessible to unauthorized users by suspending, closing, or password protecting the session prior to leaving workstation.

Workstation and network users include both Federal employees and contractors.

4.2 SYSTEMS DEVELOPMENT AND SECURITY

Many vulnerabilities exist in systems because the need for security controls is often overlooked during the systems development or procurement processes. It is generally understood that including security requirements as an integral part of procurements and systems development is the most

cost-effective approach to security. The Systems Development Life Cycle Management process must include security considerations in all its phases.

Survey Manual chapter 600.5 requires that security controls be included in the development or procurement of systems that are to process sensitive information.

4.3 TRAINING AND AWARENESS

The BITSA is responsible for ensuring that the USGS computer security awareness training program provides an opportunity for all USGS employees and contractors to obtain an overview of computer security. The program is designed to sensitize them to the need for sound security practices and provide them with an understanding of the policies, standards and procedures which govern the USGS Information Technology Security Program. The training goal is to instill and enhance a commitment in employees to actively practice effective computer security practices and protection measures. In USGS computing environments, management and technical security training become the critical foundation for managing, enforcing, and implementing USGS's Information Technology Security Program.

USGS Survey Manual Chapter 600.5 establishes the basic computer security awareness training requirements. It is important to note here that all requirements previously set forth also apply to users and administrators of networks.

Note: For employees and contractors who have access to the USGS internal Web pages, the computer security page at http://www.usgs.gov:8888/ops/computing/security contains most of the policies and guidelines previously published. In addition, the pages contain large amounts of computer security tips, recommended procedures and practices, and references to other sources of pertinent security material.

4.4 GENERAL RULES OF BEHAVIOR

This section establishes a minimum set of rules of behavior while using any U.S. Geological Survey (USGS) computer system including the networks that connect them. Managers of Federal and contract employees are responsible for ensuring that these rules are implemented in their organizations and that all users are made aware of their responsibilities. Owners of systems that require stricter rules should create them, providing these rules do not conflict or relax any of the rules set forth in this document.

Networked-based systems are inherently insecure. All users are cautioned that these technologies do not guarantee privacy. Users should not automatically expect privacy when using computers or networks and should take appropriate protective measures to protect sensitive information.

Computer Use:
Unless otherwise stated in USGS or Departmental policy, government-owned or leased computers, software, or telecommunications

systems are to be used for work related purposes only.

Passwords and User ID's:
Passwords for all USGS systems are considered private. Users are prohibited from sharing any of their system passwords. Users are responsible and obligated to select passwords that are difficult to guess to minimize the risk of having the system compromised as a result of poor password selection on their part. If exposed or compromised, passwords must be changed immediately.

User identifiers (User ID's) are required of all users for access to USGS systems. Each user must be uniquely identifiable. To ensure that access is removed, users are responsible for notifying the appropriate administrators of each USGS system on which they are registered prior to the day when they are to be separated from employment or when there is a change in their job functions that no longer requires access to a particular system or systems. When the separation is of an involuntary nature, then it is the responsibility of the employee's immediate supervisor to provide the notification(s).

User Accountability:
Users are accountable for all actions associated with the use of their assigned User ID's and may be held liable for unauthorized actions found to be intentional, malicious, or negligent.

Unauthorized Access:
Users are prohibited from accessing or attempting to access systems or information for which they are not authorized. Users are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges. Users may not imitate another system, impersonate another user, misuse another user's legal user credentials (User ID's, passwords, etc.), or intentionally cause some network component to function incorrectly. Users may not read, store, or transfer information for which they are not authorized.

Denial of Service Actions:
Users are not allowed to initiate actions which limit or prevent other users or systems from performing authorized functions including their telecommunications capability by deliberately generating excessive traffic.

Data or Software Modification or Destruction:
Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.

Malicious Software:
Users are prohibited from installing or using malicious software such as computer viruses or Trojan horses.

Authorized Software:
In general, users may only install commercial software that is

acquired through an approved USGS procurement process. Vendor licencing requirements must be followed. With approval, freeware may be installed on USGS computers where the use of such software improves the ability of employees to perform their computer-related job functions. Users are responsible for ensuring that all new software is free of computer viruses.

Reporting Computer Incidents:
Users are required to report all computer incidents (viruses, intrusion attempts, system compromises, offensive e-mail, etc.) to either their network security administrator or the Bureau IT Security Officer.

User Responsibility:
Users are responsible for following all of the above general computer use and security rules and for implementing all the appropriate controls necessary to protect the resources and information under their control. In addition, each organizational unit or system may require additional levels of security controls. Resources permitting, users are responsible for implementing any additional required controls.

4.5 PERSONNEL SECURITY

USGS Survey Manual Chapter 600.5 establishes the basic requirements for personnel security. It is important to note here that all requirements previously set forth also apply to users and administrators of networks.

In a distributed processing environment personnel security controls become increasingly important because responsibility for the protection of significant USGS assets is transferred away from centralized control into the distributed network arena. Consequently, individual users have greater responsibility for protecting those assets which compels vigorous adherence to personnel security controls.

* The USGS may impose disciplinary action for willful disregard of security policies, procedures, or a system's Rules of Behavior; violation of the Survey's employee responsibilities and Standards of Ethical Conduct regulations; or gross carelessness in handling information technology assets.

4.6 RISK MANAGEMENT

The risk management process includes the evaluation of the risks to which a system or network component is exposed and the security measures required to eliminate or mitigate those risks. The process attempts to balance the impact if a risk is realized against the operational considerations and cost considerations associated with the safeguards. Networked operating environments inherently carry with them the added vulnerabilities associated with distributing USGS information resources and their management.

* Managers of USGS organizational components that are responsible for major applications or general systems support will develop their own risk management program based on the available Federal, Departmental, and bureau guidelines and include, in their programs, the assessment of inherent risk and threats, the identification of vulnerabilities and the application of safeguards associated with computer systems. Risk assessments for major applications or general support systems (networks) must be conducted every 3 years.

Note: Guidelines for conducting risk assessments are available on the Computer Security Web Page at http://www.usgs.gov:8888/ops/computing/security/cara.html for major applications.

Guidelines for conducting risk assessments are available on the Computer Security Web Page at http://www.usgs.gov:8888/ops/computing/security/cira.html for general support systems.

4.7 SENSITIVE SYSTEM CERTIFICATION

With the revisions to OMB Circular No. A-130, all networks (LAN's , WAN's, etc.) are considered to be sensitive general support systems. Therefore, all USGS networks must be certified prior to implementation. Certification consists of a technical evaluation of network and application security controls to see how well they meet the predetermined security requirements. The security accreditation process ensures that appropriate controls have been designed into and implemented on systems. If all requirements are satisfactorily met, the information system receives "Certification" and is approved (Accredited) by the system owner, for operation. Periodic re-certifications are required.

To meet the certification requirements, a Risk Assessment and Management Control Review must be conducted for each USGS network component every three years. Following the assessment and review, a certification report on the results must be presented to the owner of the system or network for approval. System or network owners must sign certification statements indicating their acceptance or rejection of the risks associated with operating the installation or application.

Note: A sample certification statement is available on the USGS internal home page at http://www.usgs.gov:8888/ops/computing/security/certstmt.html.

4.8 SENSITIVE SYSTEM SECURITY PLANS

The completion of system security plans is a requirement of the Office of management and Budget (OMB) OMB Circular No. A-130, updated in 1996, and of Public Law 100-235. The circular does not distinguish between sensitive and non-sensitive systems. Since all federal systems have some level of sensitivity, a plan must be prepared for each. The generic term "system" is

used to mean either general support systems (networks/installations) or major applications. Existing major applications and general support systems requiring major modifications must have their plans revised prior to being considered ready for operational use. All plans must be developed using guidelines found in the NIST Special Publication 800-18, "Guidelines for Developing Security Plans for Information Technology Systems." This plan is available in PDF format (314,006 bytes), or you may download it in Microsoft Word '97 (552,448 bytes).

4.9 BACKUP PLANNING AND IMPLEMENTATION

4.9.1 NETWORK SERVERS One way to ensure that data will be around tomorrow is to back it up today. An effective backup strategy is the only way to minimize the impact of disaster related disruptions or other events that impact service availability. The goal of a backup strategy is to minimize the recovery time should data be destroyed or otherwise rendered unavailable.

The volume and criticality of the data should provide the foundation of a sound backup strategy. Network backup requirements include:

* At least one copy of all critical backup media must be removed to an off-site location. A second backup copy can be maintained in the vicinity of the system for use in recovering from a system crash;

* The frequency of backups such as nightly, weekly, monthly, or whatever period will provide for optimum recovery must be established and communicated to the users;

* The scope of the backups including complete system, incremental system backups (backup only what has changed), or individual file backups must be determined; and

* The retention periods, or time periods for which backup copies are kept as well as how many versions, or cycles, of the same backups are kept must be established.

If possible, servers should be configured to execute automatic (unattended) backup routines. Tape (or other backup media) should be properly labeled. A log of backups should exist for each server on the network. At a minimum, a weekly backup should be performed on whichever day the Administrator of the server chooses.

If backups are scheduled in an unattended mode, the workstation should be physically secured since they typically run as a Supervisor account. Leaving an unattended workstation logged on as Supervisor is risky.

Consideration should always be given to creating a permanent, off-site "archive" copy of critical data sets. This requirement is driven by records management policies and the necessity to ensure that valuable information resource assets are protected for the future.

4.9.2 WORKSTATIONS In many cases, information created and stored at the workstation level is never intended to be shared. When the only copy of the data resides on the workstation, the user must somehow ensure that backup copies are made and stored at another remote location. The remote location must be distant enough to prevent destruction of the data if something happens that damages or destroys the workplace.

* End-users are responsible for the protection of critical information stored on their workstations. Therefore, they are responsible for ensuring that copies of all critical data sets are backed up and stored at a remote location.

Today, many methods are available to the end-user for creating backups. Common methods include backing up to local media (CD-ROM, removable hard disk, digital tape, etc.) or backing up to a network server.

4.9.3 ENTERPRISE-WIDE BACKUP Since, in a networked environment, the majority of information is being stored at separate locations on either workstations or network servers, it is difficult if not impossible to know if backups are actually being made. To help alleviate this uncertainty, managers need to get involved to ensure that proper attention is paid to the retention and protection of USGS digital information. With already limited resources being dedicated to the management of distributed information systems, it is possible to achieve efficiencies by centralizing backup activities. New technologies are now available to retrieve and store critical data sets at centralized "data farms." More importantly, guarantees can be made that critical data sets will be gathered and sent to an offsite location for safe-keeping. Where feasible, organizations should combine skills and resources to implement organization-wide procedures for workstation and server backups.

4.10 CONTINGENCY PLANNING

Almost everything we do today to help us accomplish our jobs involves the use of computers. This fact alone is dramatic evidence of the tremendous importance of planning to prevent the loss of our computing capabilities. Security safeguards are employed to protect information systems resources and making preparations to easily recover from an event that damages or destroys those resources is certainly an important one of them. In fact, when all else is considered, the ability to recover may be the most effective control at our disposal.

Contingency planning provides a course of action to be followed before, during, and after the occurrence of an undesirable event that disrupts normal operations. In the past, the focus was on application or computer installation disaster recovery planning. This is still a requirement. However, the term installation has been replaced by general support systems and the definition expanded to include networks (LAN's, WAN's, Intranets, etc.). We must now ensure that local area networks and other Intranets are included in this process and that contingency plans are developed for each

USGS network component.

In addition, the definition of contingency planning must be expanded to include business recovery planning. Business functions encompass such activities as financial management, personnel, procurement and contracting, payroll, facilities management, budget and program management, etc.

The major goal of business recovery planning is to ensure that, following an event that causes an interruption of normal activities, critical business functions including the computer processing portions are successfully recovered in a reasonable time frame. This goal is not negated by changing the technology associated with the "how" and the "where" critical processing is accomplished (centralized or distributed). To the contrary, increased risks associated with a distributed computing environment make contingency planning even more of a prerequisite.

* Each organizational or functional unit of the USGS is required to either develop on their own or share in the development of a business recovery plan that addresses their network infrastructure and other asset requirements. This should be accomplished using the USGS contingency planning guidelines.

Note: Guidelines for developing network and business resumption contingency plans are available on the USGS internal Web home pages at http://www.usgs.gov:8888/ops/computing/security/cpguid.html.

4.11 MANAGEMENT OF USER ID'S

Past security audits have indicated weaknesses in our User ID management procedures. In many instances, User ID's of employees and other users of USGS systems who have left the organization or no longer need access are not purged from the system in a timely manner. Procedures for suspending or deleting User ID's and the subsequent reassigning or deleting of data sets associated with those ID's must be implemented by each system administrator. (Specific requirements are set forth in SM 600.2.)

* Network and Application Administrators have primary responsibility for managing access to their systems or applications. Each administrator must develop and implement procedures for registering and deleting users.

SECTION 5. PHYSICAL AND ENVIRONMENTAL SECURITY CONTROLS

Physical security controls focus on protecting the physical access to facilities containing USGS computer resources and the maintenance of appropriate environmental conditions. Effective physical security controls help lower the risk of the theft, damage, or destruction of USGS information resources.

Attention should also be paid to equipment awaiting installation or disposal. During this period, recommended security mechanisms are often not

in place. An effort should be made to find a temporary, secured storage area until devices are installed or properly removed from the premises.

5.1 WORKSTATIONS

Protecting workstations from theft, vandalism, or misuse creates issues not generally associated with traditional computer systems. Since most workstations are located in office environments, the responsibility for physical security must rest in the hands of the users and their managers. Although workstation users are assigned the primary responsibility for protecting their equipment and data, they must have the support of management.

* Management bears the ultimate responsibility for ensuring that sufficient resources are made available to users to provide the appropriate level of protection.

Risks associated with damage to or loss of workstations and/or peripherals vary greatly depending on various factors such as:

* Building's setting
* Local crime rate
* Single or multiple tenant building
* Area's propensity for natural hazards
* Building's physical security program

Within the building, computer equipment may be located in individual offices or open space. If equipment is located in a lockable office, then locking the office during off-duty hours is the best protection. How keys to offices and building master keys are managed is also a critical factor.

Open office space is particularly troublesome since it is generally impossible to restrict physical access to the work area. When computer equipment must be located in open space, steps such as securing equipment to the furniture with devices such as Anchor pads and cables should be taken.

5.2 CRITICAL NETWORK SERVERS

Most servers that are networked are not necessarily critical to the organization. However, there are some that are. Critical network servers are processors that provide support services that, if not available, would severely impact the organization's ability to function effectively. Such services include Web, directory services, network management for Novell, UNIX, NT, etc., or shared applications like email, time and attendance, file management, etc.

The following security measures are required for those servers that are identified as critical:

* Servers must be located in secured/restricted areas (e.g., a locked

room, continuously monitored area, or locked cabinet);

* If the servers are not located in locked rooms, the console keyboard must be locked when not in use. All network servers should be protected by either a "keyboard lock" Value Added Process, NetWare Loadable Module, or by some other physical means;

* Servers must be dedicated resources and not utilized by an individual user as a personal workstation;

* Individuals who have access to the area housing such network components should be known to the manager on-site and all members of the staff; and

* Procedures must be in place to alert system administrators when non-computer related activities are planned that may impact operations; i.e., planned power outages.

5.3 ROUTERS, BRIDGES, SHARED PRINTERS, ETC.

* Critical network devices such as routers and bridges should be treated in a manner similar to servers to ensure that they are adequately protected against unauthorized access.

5.4 CABLES, ACCESS UNITS, AND WIRE CLOSETS

* Intelligent hubs and fiber repeaters should be located in secured areas. The secured area should remain locked at all times unless the Network Administrators or an authorized repair service technician requires access to the area.

* Unused, installed cabling must not be connected to the network; thereby, providing an open access point to network resources.

* Patch cable connections to operational intelligent hubs will only be made to active workstations. When not in use, these ports should be disabled.

5.5 ENVIRONMENTAL CONTROLS

Environmental control systems include fire suppression systems (sprinklers, fire extinguishers, etc.), heating and air conditioning systems, emergency lighting, and power distribution and conditioning systems. Placing equipment and data away from the traditionally secure centralized operations center creates an additional challenge to provide the same levels of environmental protection to those resources as was provided when they were centralized.

* Servers, network interface units, and bridges should be housed in an area which is environmentally (temperature and humidity) conditioned to the extent required by the manufacturers.

* If possible, critical network devices should be consolidated and located in rooms with raised floors. Also, if the equipment is co-located, many of the above mentioned environmental controls can be implemented at a savings.

* Surge protectors should be used on all network components including individual workstations.

* Uninterruptable power supplies (UPS) are required for critical network components. UPS allows the orderly shutdown of a network service thus saving the data and work-in-process which would be lost if there was a sudden loss of power.

* Food, drink, and smoking are not permitted around the immediate vicinity of network devices.

* A fire extinguisher suitable for extinguishing an electrical fire should be present in areas where computer equipment is located. This includes office environments where PC's are located. Do not locate computer equipment near areas where combustible materials are stored.

* Smoke and water detectors should also be installed in any area where computer equipment is located.

SECTION 6. ACCESS CONTROLS

In the networked, client-server environments of the USGS, the distributed storage of sensitive data, the diverse origins of access requests, and the complicated paths which data may traverse, require effective controls over the access to USGS information resources. However, organizations that use personal computers in a strictly peer-to-peer manner for their network operations may not be able to implement some of the following mechanisms. Alternative security mechanisms such as physical access controls should be implemented to ensure information resources are adequately protected.

6.1 SECURITY MECHANISMS

USGS networked microcomputers and servers should have security controls installed which minimally include the following attributes:

* User Identification - Prior to any other action being permitted on the network, the user will be queried for a unique identification. If this user identification is not provided, no further access is allowed. The only exception granted is for accessing those few USGS hosts that are available to the general public via anonymous services.

* User Authentication - The user will be asked to verify the identity provided by offering a unique personal authenticator such as a password.

Users with high-level access privileges should be required to have more stringent authentication techniques such as token or one-time passwords. Some new authentication technologies utilize software resident on the server which works in conjunction with authentication software held by individual clients. These technologies involve the use of encryption to protect a user's access to system resources.

* Resource Access Protection (Directory, File, and Application) - Access control lists should be used to restrict access to sensitive data housed on networked devices. Users must only be given privileges based on the need-to-know and least privilege principles.

6.2 IDENTIFICATION AND AUTHENTICATION

6.2.1 USER IDENTIFICATION

* Except where noted below, all USGS system users will be required to have unique User ID's.

At present, this is one of the only ways to hold each user accountable for activities on USGS networks and systems. Within the USGS, many systems require, as the user ID, the use of some combination of the letters contained in the user's first initial and last name. To ensure the uniqueness of user ID's and to stay within a maximum number of characters allowed by those systems, last names may be shortened and other minor modifications to this sequence of characters may be made.

Groups of users (Group ID's) may be given access to a server based on specific group attributes. Providing all users with blanket access to all file servers solely for ease of configuration is not allowed.

Contract system maintenance user identifications must be approved by USGS System Administrators and rendered inactive immediately after the maintenance task is completed. User identifications developed for training need not be rendered inactive after every class if there are multiple classes during a given day, but these user identifications should be rendered inactive and reinstated at the end of the training task (i.e., training session of less than one day's duration).

Note: In organizations where applications are run on LAN's consisting of personal computers used in peer-to-peer configurations, assignment of unique user ID's may not be possible or feasible. Other alternative security mechanisms should be implemented to protect information resources.

6.2.2 AUTHENTICATION

* Passwords - At this point in time, passwords are the major mechanisms used to authenticate users' access to systems. To help ensure that the maximum access control is provided, the following procedures are required:

* Password mechanisms must be set to ensure that all passwords are a minimum six characters in length.

* USGS system administrators are responsible for establishing password expiration times for their systems. The period for resetting passwords should, in general, be based on the sensitivity (criticality) of the system.

* To minimize the chance of compromise, all users of USGS systems that require passwords shall select passwords that are in accordance with USGS guidelines for selecting good passwords. (See the Web page at http://www.usgs.gov:8888/ops/computing/security/goodpass.html for tips on selecting good passwords.)

* Administrators should implement proactive password management practices to minimize the chance of users selecting easily guessed passwords.

  Accepted practices include the use of automated front-end and retroactive password checking software, and promoting the selection and use of effective passwords as part of a security awareness program.

* Should the security requirements of a particular system indicate a need for higher levels of security, operating system or application based, automated password change features shall be implemented.

* No passwords shall be displayed on monitors during entry.

* To minimize errors during the entry of new reusable passwords, access controls shall require that they be entered twice for verification.

* Repeated, unsuccessful attempts to access a USGS system should be logged by the system and noted by the Network or System Administrators. Administrators must give serious consideration to the treatment of unsuccessful login attempts. However, limiting the number of failed attempts could lead to 'denial of user access' attacks. The best control is to deny or severely limit services such as telnet to outsiders. Except for the USGS mainframe operation where lockout is required after three failed attempts, each system administrator must establish and document their own procedures for dealing with failed login attempts. If the decision is made to lockout a user, steps must be included to confirm the identity of the 'locked out' user prior to resetting their access privileges.

* Auto-login scripts used for accessing USGS systems shall not contain the password associated with the user identification unless the entire script is encrypted. Prompting the user for the password during the login, however, is an acceptable practice.

* All passwords shall be encrypted during transmission over networks.

The transmission of passwords in plain text creates one of our greatest network vulnerabilities. With the wide-spread availability of network "sniffing" tools, it has become relatively easy to grab User ID's and associated passwords as they are transmitted over LANs or WANs.

* Passwords shall only be stored on a system using one-way encryption algorithms or hash techniques.

* Network administrators should implement system controls to set the number of generations of password permitted before a previously selected password can be reused.

* If one or more passwords have proven to have been compromised, procedures should be in place to notify the effected users, and perhaps all registered users, to immediately change their passwords.

6.3 DIRECTORY AND FILE ACCESS CONTROL

Once data is designated as a "logical" disk to a personal computer, the access control provided by the server is no longer there. For this reason, personal computers which are part of networked environments should provide some level of protection also. USGS policy states that every user of USGS systems, including networks, is responsible and accountable his or her actions associated with accessing information resources.

Data protection should be applied which employs the highest level of granularity possible. The following list represents examples of such controls.

* Access to data will be protected using the "least privilege" approach. That is: the user must be granted specific authority based on his or her need-to-know in order to read, modify, or destroy data.

* User files/directories should be owned and accessible only by the user. The user, as owner, can then grant access to other users.

* The system administrator can only grant access to user files after receiving the owner's permission. The file owner should specify the specific rights to be granted.

* Where possible, users should be treated as a member of a group and access privileges to files should be based on the group's duties and functions.

* Protection at the file level should be applied rather than at the directory level only.

* Access to network executable commands normally used for system administration should be restricted. Users should only be given the minimum set of commands necessary to do their work.

* Eliminate or severely restrict the use of 'trusted hosts'. This concept allows access to resources on other hosts (servers) without additional authentication. The ability to easily link networked hosts using this feature can open the entire intranet to attack as the result of the compromise of a single 'weak' host.

* The time and date of a user's last logon should be displayed during sign-on where operating systems permit.

6.4 APPLICATION SOFTWARE PROTECTION

Executable files should be set to "read-only" to prevent them from being modified or deleted by a user. Once applications have been loaded to a workstation, user modification of any executable programs should not be possible.

Vendors should provide, along with commercial software, the appropriate controls to restrict the number of users to that which is permitted under the terms of the site license.

Application software shall be installed to provide users with the lowest level of access needed to access and execute the application. The operating system "execute only" flag should be used whenever possible to protect application software from unlawful copying and viral infection.

* USGS system administrators shall be responsible for all host and network services software license agreements and shall ensure strict adherence to the provisions of the agreements.

* Users shall not make unauthorized copies of any licensed software.

* Users must ensure that copies of all licensed software are deleted from workstations prior to the transfer or disposal of their workstations.

SECTION 7. TELECOMMUNICATIONS CONTROLS

Telecommunications controls offer the first line of defense against unauthorized intrusions by individuals located outside the 'local' environment. However, the implementation of telecommunications controls must always be weighed against the Survey's desire to openly communicate with the public and scientific cooperators. For example, to implement gateway filters that exclude all but a select group of users, could greatly restrict our ability to continue to provide the services that our public customers have come to expect.

7.1 USGS INTERNET USE POLICY

Network resources provided by the USGS are to be used for official purposes only. In general, employees are expected to exercise common sense, good

judgement and propriety when using these government resources. The Department of the Interior has issued an internet use policy that is intended to apply to all DOI bureaus. It can be found at the following url: http://www.doi.gov/footer/doi_aup.html. In addition, the following specific rule applies:

* While using the Internet, employees or contractors are prohibited from bypassing access restrictions, subverting security controls, or otherwise impairing the functionality or availability of network resources.

7.2 WIDE AREA NETWORK ACCESS CONTROLS

USGS LAN's and workstations are connected to external networks including the Internet via gateways. The world-wide Internet has experienced a number of well publicized security problems where intruders have perpetrated attacks against government, business and academic sites. These attacks have often gone undetected and some have caused considerable general mischief and cost to the victim organizations. However, the Internet serves millions of users and provides valuable services such as remote system access, file exchange, electronic mail, and other information resource services. There are numerous benefits to world-wide Internet access when it is used in a secure manner.

The Department of the Interior maintains a wide area Intranet called DOINET. This WAN serves the entire Department, nationwide and provides Internet connectivity. The DOINET security policy states that no additional security is provided by DOINET. It is the responsibility of each bureau that uses DOINET to provide security controls for each connected host.

However, DOINET is not the only way that we connect to the Internet. It is important that, at any point where a connection is provided to the Internet, we ensure that appropriate security controls are implemented to protect our internal computer resources.

7.2.1 FIREWALLS

A 'firewall' is a security mechanism used to protect an intranet from the other untrusted portions of the Internet. In the most general sense, a firewall can be used to screen and govern traffic. This ability helps resist a large number of attempted attacks from external sources and provides considerable leverage with respect to network security. However, careful consideration must be given prior to implementing a firewall since they can severely restrict the normal flow of telecommunications traffic in to and out of an intranet. In the USGS, the strong desire to promote open communications with cooperators and customers makes the implementation of firewalls a particular challenge.

* Prior to implementing a firewall, a service-access policy that defines exactly what services the organization makes available to entities outside the intranet must be established.

Firewall designs offer three basic options, each with their own advantages and disadvantages.

Packet-filtering. Filtering can block connections from or to specific hosts, networks, or ports. Packet-filtering is the simplest and most common form of firewalls. A site can, for instance, block connections from certain addresses considered as untrustworthy. A packet-filtering router could also restrict internal users to only selected systems and services outside the organization. Packet-filtering provides little or no logging and could require extensive resources to manage the complex filtering rules.

Circuit-level gateway. This type of firewall provides greater control over Internet traffic than a packet filter, but is more expensive. A circuit-level gateway determines the nature of each connection from an external host to a host on the intranet. Since they function at the transmission layer, more complex security policies can be implemented including user identity and time of day.

Application gateways. This type of firewall uses software applications to forward and filter connections for services such as Telnet, FTP, and HTTP. Such an application is referred to as a proxy server or application gateway. The key difference between a packet-filtering router and a proxy server is the proxy server's ability to filter and log at the application level of the OSI model rather than just the IP level. Application gateways can also hide internal host names and IP addresses and provide robust authentication.

7.2.2 Firewall Guidelines

Any installed firewall should have the following attributes:

* The firewall should support (not impose) a policy of denying all services except those specifically permitted.

* The firewall implementation should be flexible to accommodate technological and organizational changes.

* It should employ filtering techniques to deny services to specific host systems

* It should accommodate public access to the site, when appropriate. Public Access to some USGS sites may be denied through the use of firewalls.

* It should concentrate and filter dial-in access.

* It should log traffic and suspicious activity.

* Only a secured version of the firewall host's operating system should be installed. It should be carefully configured to ensure that it can

not be broken into and used to penetrate USGS hosts.

* At a minimum, all USGS gateways to the Internet must provide filtering to minimize the threat of an outside host masquerading as a host with an internal IP address.

7.3 DIAL-IN ACCESS CONTROLS

Access to an Intranet which has no communications connections to the outside is generally limited to those with access to the facility itself. Once dial-in (remote) access to a local area network is provided, the vulnerabilities increase and additional controls are needed to protect the Intranet. Dial-in access capabilities are technically possible to a microcomputer or directly to a network server if the server has been equipped with a dial-in port. The calling computer requires only communication software, a modem, a telephone line and the network dial-in number to complete the connection.

Even though network dial-in capability is intended strictly for authorized users only, dial-in capabilities increase the risk of unauthorized access.

Except for USGS-provided public-accessible Web services, the following controls are required when remote, dial-in access to the USGS Intranet is provided:

* All remote access users must be required to register for access. As part of the registration process, users must be reminded of their responsibilities to protect USGS information resources and the penalties for abusing their privileges;

* Controls must be implemented at each access point to authenticate each user (Unique User ID and password);

* All standard access controls required for other USGS systems must also be implemented for dial-up (i.e., minimum password length, automatic password expiration dates, limit failed log-in attempts, encrypted password files, maintain access logs, etc.);

* System description information in opening banners must be restricted to an absolute minimum;

* Standard warning banner regarding unauthorized use and possible monitoring activities must be displayed;

The following additional controls are recommended when dial-in access to the USGS Intranet is provided:

* Call-back features should be used when possible;

* Avoid using the same modems and phone lines to be used for both dial-in and dial-out. This is to help prevent callers from using the

modem pool as part of chain of logins;

* Be sure modems can't be reprogrammed while in service;

* Program modems to either reset at the start or end of each call.

7.4 REMOTE SYSTEMS ADMINISTRATION

In a networked environment, system administrators are exposed to many threats. One such threat deals with the use of 'sniffer' software by an intruder to gain unauthorized access. 'Sniffers' are programs designed to view and collect packets traveling over the networks and are readily available from Internet sites around the world. 'Sniffer' software has been responsible for many successful break-ins. An intruder who gains access (root privileges) can plant a 'sniffer' package and gather the login information of any other user connected to that segment of the network. Logical devices such as bridges can be used to isolate and thereby limit the extent of this threat.

* System administrators, when using administrator privileges to access their hosts from a 'remote' terminal, must protect their system authentication through the use of either a direct connection (hard-wired coaxial cable) or encryption.

7.5 USE OF NETWORK ANALYSIS TOOLS

Network protocol analyzers, often referred to as 'sniffers' are used to collect, analyze, and display data running on a network. These tools capture and display "all" information transmitted over a network including the source and destination of the data and identifiers such as passwords and ID's. They are also capable of building databases of all network devices, storing network activity information and data on disks, and even generating its own data that can block selected networked devices and artificially load the network.

Network analysis tools used to come packaged in the form of an expensive laptop computer with all necessary proprietary software loaded. The only exception was the Sun workstation which could be turned into a sniffer by simply altering the ethernet card to capture all the data. Since then, network analysis software has come into the public domain providing anyone with the ability to observe and even steal information traversing networks.

Network analysis tools can be invaluable for troubleshooting, when used properly. These programs save considerable time in tracking down and dissecting network problems. However, in the hands of individuals determined to gain unauthorized access to systems, this software can make it an extremely easy task. The best way to protect against the illicit use of network analysis software is to implement encryption.

The following controls on the use of network analysis software are viewed as minimum requirements:

* Authorized use of network analysis software is restricted to officially designated system, network, or security administrators;

* Unauthorized use of network analysis software may result disciplinary action (unauthorized use includes 'sniffing');

* Except when approved by the particular network security administrator, no network analysis tool shall remain connected to a network for an indefinite period.

SECTION 8 ENCRYPTION

Data encryption provides one of the highest levels of security possible. It protects data during transmission across networks or when stored on magnetic or optical media. Encryption may be applied at any point during the data creation or transmission process and can be accomplished using hardware devices or software. Where it is applied, depends on the requirements for confidentiality (privacy) and integrity.

In the Survey Manual Chapter 600.5.5, sensitive data is described as any data that requires additional protection due to the risk and magnitude of the loss resulting from inadvertent or deliberate disclosure, alteration, or destruction. Sensitive data include proprietary data, records about individuals requiring protection under the Privacy Act, financial data including payroll information, or any other data declared to be critical to the mission of the USGS. Any system generating, transmitting, or collecting (storing) such information must be declared sensitive.

* The use of encryption is required to protect user authentication when accessing any USGS system and especially any information that, if disclosed, would violate the privacy of any customer, employee, or contractor.

* Encryption should be used to protect sensitive data during transmission over USGS networks and the Department network (DOINET). Encryption must be used when transmitting sensitive data over the Internet.

Encryption is achieved through the use of an algorithm that transfers data from its readable form to cipher. An algorithm is a complex mathematical formula that defines the operation. The operation is controlled by a 'key'. Keys are randomly generated strings of bits that are used to create and unlock the cipher. Reversing the encryption process and transforming the cipher back to its form is called decryption. Encryption and decryption comprise the science of cryptography.

In order to "recover" the data, decryption algorithms utilizing the same key must be used. The two types of keys most commonly used for encryption are the secret-key and the public-key. Secret-key encryption means that all persons involved in the exchange of data must know the key. It is the most

efficient form but requires considerable management and distribution and is inappropriate for casual use.

Public-key encryption divides the key into public and private halves. The private half is known only to the individual using it, and the public half of the key is provided to a restricted target community.

Encryption key management (key escrowing) is central to the success of protective measures that depend on encryption. It is apparent that, as the use of encryption increases in the USGS, a key-management structure must be developed to help guarantee the privacy and recovery of keys and to prevent the spread and use of incompatible encryption standards. Key-management can be accomplished through a contract with one of the commercial vendors who provides such services or by establishing a key-management function within the USGS.

8.1 ENCRYPTION STANDARDS

There are a number of encryption standards. An encryption standard is determined by the structure of the key used to encrypt and decrypt. The Data Encryption Standard (DES), published by NIST as Federal Information Processing Standard (FIPS) 46-2, is the best known secret-key system. DES is currently the only secret-key standard officially approved for use by Federal agencies. However, Federal agencies are beginning to purchase commercial products which are based on algorithms that use much longer keys.

The DES was adopted in 1976 and, because no viable replacement was found, was recertified last in 1993. A variation of DES is Triple-DES. This mechanism encrypts the message with DES three consecutive times, using a different key for each encryption. Its 112-bit key consists of two independent 56-bit keys. It is currently considered to be the most secure method for encryption.

There are several public-key encryption standards. RSA is a public-key algorithm developed in 1978. The 512-bit keys are generated mathematically by combining or factoring large prime numbers. RSA provides authentication in addition to encryption, thus assuring the recipient that the message comes from the purported sender. RC2 and RC4 are proprietary algorithms. They have variable key lengths and have been given special export approval by the U.S. government as long as their key length is 40 bits or less. They are being used in commercial E-mail products. Generally speaking, vendor-proprietary algorithms should be avoided since they have not been tested via peer review.

Questions have been raised recently regarding the strength of the DES standard since it is based on a relatively short 56-bit key. There have been claims made that DES and RSA have both been broken. But it must be assumed that, since huge resources are required to accomplish this, using either of these algorithms would be acceptable for our needs.

8.2 IMPLEMENTING ENCRYPTION IN THE USGS

It is the intent of the USGS to discourage the uncontrolled or uncoordinated implementation of encryption products. Although commercial products for electronic mail and Web services now provide encryption options, they also may use different standards.

* The USGS will have a single, centralized management structure to support the use of a common encryption standard for non-classified systems and data.

The only exception to this policy is when encryption is required by another Federal agency such as Treasury or other customer to transmit sensitive information using a standard dictated by that agency or customer.

Controlled implementation and use of encryption in any organization is based on the establishment of Certificate Authorities. A Certificate Authority (CA) is a trusted third party whose job it is to check and certify the authenticity of users or services. The CA is responsible for issuing the digital certificates (keys) to only those entities, users or services, which have been validated. Digital certificates can be used to secure sessions with server, establish the authenticity of the server or, in their most comprehensive form, authenticate clients (users).

* To help ensure that encrypted communications is possible between all organizations of the USGS, all requests for the non-classified use of encryption products must be made through the BITSA.

* The BITSA will be responsible for obtaining and distributing digital certificates for USGS computer services and users.

SECTION 9 USGS WEB SERVICE SECURITY

9.1 INTRODUCTION

The World Wide Web (WWW) holds great potential for providing information to the public more quickly and efficiently than has ever before been possible. The remarkable growth in the number of Web servers, the amount of information they contain, and their use by the public contribute to making the Web the single, most important information dissemination mechanism for the USGS. These facts intensify the need to establish sound security standards and guidelines for USGS Web services.

9.2 RISKS ASSOCIATED WITH WEB SERVICES

While the vulnerabilities and risks discussed here apply to any host connected to the Internet, the focus of this section is on USGS hosts that provide Web services. The main reason for this emphasis is because Web servers are a favorite target of hackers.

One of the major risks to Web service providers is that someone might be

able to fool their server deamon software into doing something it is not supposed to do, thus allowing an attacker to break into their server and do some harm. The harm might include planting Trojan horses in files being provided to clients, corrupting other server information, gathering data about users and their system access, releasing information from the server, or using the server as a platform to launch attacks against other machines.

Since we now depend heavily on our Web servers for the continuous dissemination of information, the risk of denial-of-service attacks has more significance. These attacks usually consist of attempts to bring the Web server down or to overload it so that it can no longer respond to connections from browsers. This can occur at the TCP/IP level, such as automated routines that ping the server's IP address incessantly, or through scripts that constantly access large files from the server. Denial-of-service attacks tend to be short-lived and are usually the result of some reaction to publicity about the targeted organization.

9.3 TYPICAL WWW SERVER VULNERABILITIES

Server vulnerabilities vary from operating system to operating system. However, two general areas of vulnerability potentially affect all WWW servers. These are:

* The server may allow access to files located outside the file area designated for WWW access. Intruders may be able to trick some HTTP servers into returning system files such as the password file.

* Most HTTP servers support executable scripts (Common Gateway Interface, or CGI, scripts) that compute information to be sent back to remote users at the time of demand. THIS IS THE AREA OF GREATEST VULNERABILITY FOR AN HTTP SERVER. The system often cues these scripts using input from remote users; this information is generally supplied via a fill-out form. If these scripts are not carefully written, intruders can subvert the scripts to execute arbitrary commands on the server system.

9.4 SECURE SERVER DESIGN

9.4.1 SECURITY GOALS FOR WEB SERVICES

In order to minimize the risks associated with Web servers, while still providing a commercial presence for these services to the Internet community, an appropriate level of security controls must be implemented. The goals of this effort are to achieve:

* Information Integrity: We want to assure that the information residing in the server is not corrupted by the actions of legitimate or illegitimate clients as a result of their use or abuse of the service.

* Availability of Service: We want to assure that clients cannot make the server unuseable for other clients as a result of their use or

abuse of the service.

* Confidentiality: We want to assure that the service only provides information to clients that is explicitly authorized for outside use.

9.4.2 SERVICE TYPE AND LEVEL OF ACCESS

For the purpose of establishing a reasonable set of security controls, the type of Web service that will be provided and the requisite level of access control for each must be defined. All USGS Web services will classified as to type based on one of the three services listed and the appropriate access controls.

* Public: A public Web service is one that is open to public access. Any user will be granted unrestricted access to the information contained on that server.

* Internal: Internal use Web services provide what are generally referred to as Intranet services and are available to USGS employees, contractors, cooperators, and individuals. Access to internal services is restricted to IP addresses within the usgs.gov domain and to other authorized and authenticated customers.

* Restricted Internal: Restricted internal Web services are used primarily for sensitive administrative applications (e.g., Automated Time and Attendance system), internal research projects, service testing, or product development. Access is password protected and controlled by a mechanism such as .htaccess.

9.4.3 SECURITY REQUIREMENTS FOR USGS WEB SITES

To meet the security goals stated above and to help guarantee that the desire to provide Web services to the public does not increase the level of risk associated with Internet access, the USGS must have an effective Web Security Certification Program. The critical components of this program are: policy, implementation, and monitoring. The USGS policy on Web implementation is:

* Prior to being designated as an official, publically available USGS Web site and to permitting unrestricted access by the public, the service must receive a security certification. For the service to be certified, all required security controls and available system patches must be implemented, tested, and approved by a designated certifying official.

Below, is a detailed description of the recommended minimum security controls required for the various types of USGS Web sites.

All Server Types: The following security controls are required for all USGS Web sites.

* All currently available patches for known system vulnerabilities must have been installed. The site administrator must also agree to install new patches as they are made available.

* The server daemon for all Web services must be run as a non-privileged user rather than as user 'root' or 'administrator'.

* System audit-logging capabilities must be enabled for all Web servers. The level and detail is at the discretion of the system administrator.

* CGI scripts must be written to avoid passing remote user input directly to command interpreters on all Web servers. They should not be run nor located in the user's home directory.

* Services providing information about the system's users, such as 'finger' and 'rusers', should be disabled.

* Monitoring and access control tools such as 'logdaemon' and 'tcp wrappers' should be installed on UNIX servers. Equivalent monitoring tools must be installed on NT Web servers.

* Shadow password files or equivalent mechanism for protecting password files and utilities that disallow poor passwords must be implemented. System administrators should use utilities such as 'Crack' to check password files.

* All unused or dormant accounts must be disable or deleted.

Internal Access Servers: In addition to the controls listed in the section above, systems providing internal access web services must:

* Restrict access to authorized systems and users (.htaccess).

  Strictly limit the use of NIS.

  Strictly limit the use of NFS mounts and exports.

Internal-Restricted Servers: In addition to the controls listed in the above two sections, systems providing Web services for sensitive applications, testing, product development, etc. must:

* Restrict access to authenticated users (.htpasswd).

Public Web Servers: In addition to all of the above controls, Web services that provide unrestricted access to the public must:

* Be logically isolated from the USGS Intranet by placing them on a separate subnet.

* Run on a dedicated server; that is, no other services except those used to support the primary Web service should be loaded.

* Not permit the export of files.

* Not permit the mounting of remote file systems.

* Not implement Network Information Services (NIS).

* Not permit the use of user's '.rhost' or systems 'hosts.equiv' files.

* Ensure that the system password file only contain the id's of those who administer the server.

* Encrypt all remote logins for system administration.

9.5 WEB SECURITY MONITORING

The BITSA is responsible for ensuring that an effective USGS Web service security monitoring program is in place. It is the responsibility of the Bureau IT Security Office to conduct periodic site security scans of all USGS hosts running Web services to determine the status of Web security and to ensure that only certified sites are listed as official USGS Web sites on the USGS Home Page. At the recommendation of the BITSA, USGS managers and supervisors are responsible for supporting the suspension of Web services that are not in compliance with the security requirements contained in this section.

SECTION 10. VIRUS CONTROL

10.1 NETWORKS

Networks facilitate the easy exchange of data. Unfortunately, the ease of data interchange is not limited to legitimate data; it also enables the spread of computer viruses. The fundamental requirement for a virus to be able to infect a server is for it to have the write and/or create privilege. Viruses spread between workstations by infecting executable files. The more users sharing the executable, the more widespread the infection. If a common executable (e.g. login on NetWare) becomes infected, the virus can spread to most workstations on the network within minutes.

To successfully minimize the risk of virus infections on networks, two steps can be taken:

* Minimize write/create access rights. The existence of users with write/create access rights will leave security gaps. Network Administrators must establish which users have the need for write/create rights and to which areas. Read-only areas should be established where executables are stored.

* Implement early virus detection. Efficient virus detection procedures must be established. The earlier a virus is detected and dealt with, the less chance it has to spread. The preferable location for early

detection is at the workstation, but the installation of anti-virus software on network servers will minimize the risk of propagation and introduction from the outside.

10.2 INDIVIDUAL WORKSTATIONS

Virus protection on individual USGS workstations must rely on the awareness and vigilance of the users who are operating personal computers attached to the LAN. Personal computer users are, in effect, system administrators and must engage in sound management practices to protect their software and data from infection by malicious software.

USGS network users must assume the responsibility for providing a virus protection capability for their own workstations.

Workstations should be configured to execute a virus monitoring program upon start-up. It is highly recommended that this program remain resident while the workstation is operating. A check for viruses or other unauthorized programs should be performed prior to backing up to file servers.

New software should be checked for viruses prior to being loaded on PC's. Two types of scanning should be employed: virus signature-based scanning that can precisely identify specific viruses; and integrity based scanning that can detect whether program files have changed in content, size, or date from the original snapshot of the program.

Users with PC or MAC workstations attached to USGS networks should:

* Periodically check their personal computers for virus infections with accepted virus prevention and detection software;

* Not upload executable programs into public storage areas of LAN servers;

* Be alert for unexpected changes in the performance of their personal computer or other abnormal behavior;

* Never load software or data onto their personal computers from diskettes which have not first been subjected to scanning for malicious software. Be especially careful of boot sector viruses. Some viruses travel from personal computer to personal computer in the boot sector of floppy disks. If an infected disk is left in the 'A' drive of a personal computer and the machine is turned on, the virus will spread to the hard disk even as the "non-system disk" error appears on the screen;

* Change the workstation startup routine so that it looks for the C drive first and then the CD rom drive (if applicable) during the boot process. This will prevent an infected disk, left in the A drive, from infecting the system.

* When files are downloaded from external (untrusted) sites via modem or the network, they should be scanned prior to saving to the hard drive;

* On a regular basis, backup all non-executable files residing on the personal computer;

* Report all suspected malicious software incidents to their immediate supervisor, LAN administrator, or Bureau Automated Information Systems Security Administrator (BITSA).

* Scan files prior to including as email attachments.

10.3 COMPUTER VIRUS ALERTS

Announcing to the user community the threat of a computer virus occurrence that could impact a large number of computers is a serious matter. The source of such announcements must be trusted. The source must be trusted to know what is real or simply a 'hoax'. Computer virus 'hoaxes' have caused a great amount of concern to USGS PC users. This is mostly because individuals have taken it upon themselves to forward the 'false' notification to friends and coworkers without verifying the validity of the warning. On-the-other-hand, there have been occasions (very infrequent) when computer virus alerts were necessary because of an imminent, real threat. We must be ready to react properly if they occur again.

* The only authorized source of a general (bureau-wide) computer virus alert in the USGS shall be either the BITSA or the USGS Incident Response Team. (See Section 11.3.)

SECTION 11 INCIDENT RESPONSE AND REPORTING

11.1 INTRODUCTION

OMB Circular A-130 requires that all Federal agencies develop and implement a Computer Security Incident Response Capability (CSIRC). This requirement resulted from the drastic increase in the number of incidents involving the penetration, compromise, and misuse of government computers. Computer incidents can take on many forms. They include such acts as:

* breaking into a computer and gaining control for unauthorized activities;

* flooding the communications ports with data packets to deny access to other users;

* modifying the home pages of government Web sites;

* forging email messages;

* planting malicious code such as viruses and Trojan Horses; or

* soliciting child pornography or distributing hate mail.

Traditional security controls like risk analysis, contingency planning, and security reviews have not been sufficient in controlling incidents and preventing significant damage. However, a CSIRC, when combined with these traditional computer security elements, can provide bureau-wide protection from possible damage to its information technology resources and its reputation.

11.2 CHARACTERIZING AN INCIDENT RESPONSE CAPABILITY

The USGS must be in a position to respond quickly to computer security incidents to minimize their impact and recover in a timely manner. A CSIRC should be a combination of technically skilled people, policies, and procedures that constitute a proactive approach to handling computer security incidents. An effective CSIRC has the following characteristics:

* Immediate: Immediate response means that the response to incidents and announced threats should be as soon as is reasonably possible so that damage to bureau IT resources can be minimize. With the available resources, it may not be feasible to provide 24x7 service.

* Centralized: Centralized means that management and coordination functions should be located at USGS headquarters and closely associated with the USGS Help Desk.

* Consistent handling: Consistent implies that any group calling itself an Incident Response Team (IRT) must react to security incidents or threats in the same, uniform manner each time. The USGS user community must agree that the consistent treatment of incidents are in its general interest. To help ensure this, IRT services must be clearly defined.

* Coordinated: Coordinated means that all activities associated with incident response are accomplished with full cooperation of the designated representative(s) from the affected organizational unit.

* Educational: Educational implies that there is something to be learned and shared from each incident. The IRT should make available to the user community all current incident awareness information via the USGS computer security home page.

11.3 USGS INCIDENT RESPONSE CAPABILITY REQUIREMENTS

The following is a list of requirements that the USGS computer security incident response capability must meet:

* The primary functions of the USGS CSIRC shall be to: provide security-related advisories and alerts; to conduct network and host vulnerability analyses on a routine basis; to conduct analyses of

problems (incidents) including their magnitude and impact; to provide technical advice and assistance to the user community; to coordinate all activities with the user community; and to report significant incidents to the appropriate Federal officials.

* The USGS CSIRC must be part of the overall USGS computer security program. This activity shall be under the direction of the BITSA.

* The IRT shall be composed of the BITSA, a full-time computer specialist, and representatives from each of the divisions and/or the regional offices.

* The IRT is currently authorized to manage response to security incidents that involve sites within the domain of usgs.gov. The group may also, upon request, provide support to other Department organizations.

* The IRT shall coordinate all computer security-related incident response activities with the appropriate affected organizational units.

* The IRT shall have sole responsibility and full authority to deal directly with outside entities including representatives of the CERT, law enforcement officials, the OIG, and if appropriate, the individuals or organizations responsible for the unauthorized activities.

* All users and USGS designated IT officials are required to report all computer security incidents (see Section 11.1 for types of incidents) to the IRT for appropriate action.

* The IRT must operate under an approved charter.

* All incidents shall be documented and must include all information as described in the Charter.

11.4 INCIDENT REPORTING

Computer security-related incidents can range from a minor, one-time computer virus infection of a single machine to an event involving unauthorized intrusions into a number of a network hosts. Although all incidents are to be reported, the level to which an incident is raised is a judgement call on the part of the local system administrator. If the event can be dealt with locally and the impact (number of machines or users involved, cost to repair damage, etc.) on the organization is minimum, then a report to the BITSA stating the details of the event and what was done to correct the problem is all that is required.

Note: Information on how to file an incident report can be found at the following Web location:
http://www.usgs.gov:8888/ops/computing/security/irarticl.html

U.S. Geological Survey, MS 807, National Center, Reston, VA 22092, USA
URL http://www.usgs.gov:8888/ops/computing/security/hndbk3.html
Last modification: 28 Jun 1999@10:06

SYSTEM ACCESS REQUEST

Forward this request to the CSB Support Services Help Desk, Computer Operations.

Statement of Accountability

My signature acknowledges that I:

- ♦ Am responsible for actions performed through my user-id.
- ♦ Must have a password associated with my user id that is known only to me.
- ♦ Will change my password as mandated, and if I believe my password has been compromised, I will change it immediately and notify the ADP Security Officer, in order to protect the security of EDC=s computer systems.
- ♦ Knowingly risk disciplinary action if I do not comply with security procedures.

Signature of Requestor:_____ Phone Number _____ Dept _____

Printed name of Requestor:_____ Date: / / Employee ID#_____

__ Government __ Contractor Contractor Name:_____

Access Needed

__ UNITREE
__ NetBlazer
__ Cisco RAS (PPP)
__ EDCFTP
__ WINDD
__ Windows NT
__ Novell/Groupwise
__ Groupwise Distribution List(s) required for this user: _____
_____

Printer preference_____

EDC System/Workstation (example SG1 SGW1)

__ Silicon Graphics _____
__ Data General _____
__ Sun _____

__ Oracle _____

Oracle System ID(s) Role(inquire, maint. full)
_____ _____
_____ _____
_____ _____

EDC User-id affected:_____ Action: Add___ Delete___ Change___

Oracle User-id affected:_____ Action: Add___ Delete___ Change___

Expiration Date:__/__/__

Chargecodes/Mnemonics to be accessed:_____

Manager or TAL Concurrence

Approved by:_____

Project Leader Concurrence

The Task numbers/Chargecodes accessed above are appropriate.

Approved by:_____

FOR HELP DE[illegible] USE ONLY

Date Comple[illegible]d: __/ __/ __ Completed by_____

Ronald A. Parsons ADP Security Officer (605)594-6555 April 1998

Appendix C - Router Specification Sheets

Specifications

Dimensions and Weight

4-Slot Chassis
Length: 40.4 cm/15.9 in
Width: 44.2 cm/17.4 in
Height: 13.5 cm/5.3 in
Weight: 13.6 kg/30.0 lbs

8-Slot Chassis
Length: 42.4 cm/16.7 in
Width: 44.2 cm/17.4 in
Height: 18.5 cm/7.3 in
Weight: 22.7 kg/50.0 lbs

8-Slot Extended Chassis
Length: 49.2 cm/19.4 in
Width: 44.2 cm/17.4 in
Height: 53.3 cm/21.0 in
Weight: 42 kg/91 lbs (one power supply) 50 kg/109 lbs (two power supplies)

Dual Power Supply for 8-Slot Chassis
Length: 41.3 cm/16.25 in
Width: 44.2 cm/17.4 in
Height: 13.0 cm/5.1 in
Weight: 12 kg/27 lbs

NETBuilder II WAN Extender
Length: 43.9 cm/17.3 in
Width: 38.9 cm/15.3 in
Height: 4.3 cm/1.7 in
Weight: 4.7 kg/10.3 lbs

Power Requirements

4-Slot Chassis
90-120 VAC, 4763 Hz, 2.3 A 180-264 VAC, 4763 Hz, 1.4 A 117 W

8-Slot Chassis
90-120 VAC, 4763 Hz, 4.1 A 180-264 VAC, 4763 Hz, 1.4 A 170 W

8-Slot Extended Chassis
90-132 VAC,47-63 hz, 12.3 A max. 180-264 VAC,47-63 hz, 6.2 A max. 700 W

Environmental Ranges

4-Slot and 8-Slot Chassis
Temperature: 41° to 104° F (5° to 40° C)
Humidity: 20% to 80% noncon-densing

8-Slot Extended Chassis
Temperature: 32° to 122° F (0° to 50° C)
Humidity: 10% to 90% noncon-densing

Thermal Rating

4-Slot Chassis
Max. output: 400 BTU/hour

8-Slot Chassis
Max. output: 580 BTU/hour

8-Slot Extended Chassis
Max. output per power module: 1389 BTU/hour

Noise Level

4-Slot Chassis
48.5 db at 1.5 m 50.6 db at 1 m

8-Slot Chassis
46.5 db at 1.5 m 48.5 db at 1 m

8-Slot Extended Chassis
One Power Supply 42.5 db at 1.5 m 44.0 db at 1 m
Two Power Supplies 47.4 db at 1.5 m 46.5 db at 1 m

Reliability

Mean Time Between Failures (MTBF)
Based on MILSPEC (217.E) at 25° C

Product	MTBF (hours)
NETBuilder II WAN Extender	20,190
Communications Engine Card (CEC)	67,809
ATM UNI	286,000
FDDI Module MAC	98,704
FDDI Module PHY	107,182
Ethernet Module	227,469
Ethernet 2-Port 10BASE-FL Module	195,238
MP Ethernet 6-Port 10BASE-T Module	110,000

MP Ethernet 6-Port 10BASE-FL Module 128,000
Fast Ethernet 100BASE-TX Module 344,823
Fast Ethernet 100BASE-FX Module 362,000
Token Ring+ Module 309,761
HSS Module V.35/RS-232 167,195
HSS Module RS-449 240,774
HSS Module G.703 287,891
HSS 3-Port V.35 Module 119,000
HSS 3-Port RS-232 Module 104,000
HSS 3-Port RS-449 Module 97,000
HSS 3-Port X.21 Module 97,000
HSSI Module 120,000
4-Slot Power Supply 82,413
8-Slot Power Supply 103,495
8-Slot Extended Power Supply 112,000
Flash Memory Drive 650,280
Floppy Disk Drive 30,003
Front Panel Card 1,032,268
Backplane 2,333,558

Mean Time to Repair (MTTR)

Time to mechanically replace each of the components listed, assuming fault isolation has taken place.

Product	MTTR (minutes)
Communications Engine Card	<1
Interface Modules	<1
4-Slot Power Supply	<30
8-Slot Power Supply	<5
8-Slot Extended Power Supply	<1
Flash Memory Drive, 8-Slot Extended Chassis	<1
Floppy Disk Drive, 8-Slot Extended Chassis	<1
Front Panel Card, 8-Slot Extended Chassis	<5
Flash Memory Drive, 4- and 8-Slot Chassis	<30
Floppy Disk Drive, 4- and 8-Slot Chassis	<30
Front Panel Card, 4- and 8-Slot Chassis	<30
Backplane	<90

Supported Standards

IEEE Standards
802.1d MAC Bridging
802.1e System Load Protocol (SLP)
802.1i MAC Bridges FDDI Supplement
802.1d, IBM Token Ring Annex C Architecture (source route bridging)

IEEE Recommended Practice

P802.h MAC Bridging of (proposed) Ethernet Version 2.0 in 802 LANs

ANSI Standards

X3T9/90 FDDI Station Management (SMT) Revision 6.2/7.3
T1/S1, Standards for T1.617 Frame Relay Link Annex D Management Interface

ITU-T (CCITT) Standards

I.430 Basic user-network interface--Layer 1 specification
Q.921 ISDN user-network interface--Data Link Layer specification
Q.922 Frame Relay Annex D
Q.2110 Broadband Integrated Services Digital Network (B-ISDN) ATM Adaptation
Layer--service specific connection oriented protocol (SSCOP) per ATM UNI 3.1
Q.2931 Broadband Integrated Services Digital Network (B-ISDN) Digital subscriber signalling
system no. 2 (DS52) user network interface layer 3 specifications for basic cell/connection control
per ATM UNI 3.0, 3.1
Q.931 ISDN user-network interface-- Layer 3 specification for basic call control
X.3 Packet Assembly/ Disassembly (PAD) facility in a public data network
X.28 DTE/DCE interface for start/stop DTE accessing a PAD
X.29 Exchange control information and user data between a PAD and DTE or PAD
V.25bis Automatic call/ answering signaling interface on general PSTN

Internet Standards

RFC 768 User Datagram Protocol (UDP)
RFC 783 Trivial File Transfer Protocol (TFTP)
RFC 791 Internet Protocol (IP); equivalent to MIL STD 1777
RFC 792 Internet Control Message Protocol (ICMP)
RFC 793 Transmission Control Protocol (TCP); equivalent to MIL STD 1778
RFC 826 Ethernet Address Resolution Protocol (ARP)
RFC 827 Exterior Gateway Protocol (EGP)
RFC 854 Telnet
RFC 855 Telnet option specification
RFC 856 Telnet binary transmission
RFC 857 Telnet echo option
RFC 858 Telnet suppress go ahead option
RFC 888 Exterior Gateway Protocol (EGP)
RFC 894 IP datagrams over Ethernet networks
RFC 903 Reverse ARP RFC 904 Exterior Gateway Protocol (EGP)
RFC 906 Bootstrap loading using TFTP

RFC 919 Broadcast Internet datagrams
RFC 922 Broadcast Internet datagrams in the presence of subnets
RFC 950 Internet standard subnetting procedure
RFC 951 Bootstrap Protocol (BootP)
RFC 959 File Transfer Protocol
RFC 1009 Requirements for Internet gateways
RFC 1027 Proxy ARP
RFC 1034/5 Domain names
RFC 1042 IP datagrams over IEEE 802 networks
RFC 1058 Routing Information Protocol (RIP)
RFC 1108 Revised IP security
RFC 1122 Requirements for Internet hosts (routers)
RFC 1141 Incremental updating of the Internet checksum
RFC 1155 Structure and identification of MIBs
RFC 1156 MIB I
RFC 1157 SNMP
RFC 1188 IP datagrams over FDDI networks
RFC 1191 Path MTU discovery
RFC 1195 Use of OSI IS-IS for routing TCP/IP
RFC 1209 Transmission of IP datagrams over SMDS
RFC 1212 Concise MIB definitions
RFC 1213 MIB II (with extensions)
RFC 1220 PPP extensions for bridging
RFC 1231 Token Ring MIB
RFC 1236 IP to X.121 address mapping for DDN
RFC 1243 AppleTalk MIB
RFC 1247 OSPF version 2
RFC 1253 OSPF version 2 MIB (with extensions)
RFC 1256 Router Discovery
RFC 1236 Defense Data Network (DDN)
RFC 1271 RMON MIB, alarm and event groups
RFC 1284 Ethernet-like MIB
RFC 1285 FDDI MIB (with extensions)
RFC 1286 Bridge MIB (with extensions)
RFC 1293 Inverse ARP
RFC 1304 SMDS MIB
RFC 1315 Frame relay DTE MIB (with extensions)
RFC 1332 PPP Internet Protocol Control Protocol (IPCP)
RFC 1334 Password Authentication Protocol (PAP): Challenge Handshake Authentication Protocol (CHAP)
RFC 1338 (Supernetting) CIDR
RFC 1347 TCP and UDP with Bigger Addresses (TUBA)
RFC 1350 TFTP revision 2 (obsoletes RFC 783)
RFC 1354 IP forwarding MIB
RFC 1356 Multiprotocol Interconnect on X.25 and ISDN in packet mode (obsoletes RFC 877)

RFC 1376 PPP DECnet Phase IV Control Protocol
RFC 1377 PPP for OSI network layer control
RFC 1398 Ethernet MIB
RFC 1434 Data Link Switching (DLSw)
RFC 1483 Multiprotocol encapsulation over ATM Adaptation Layer 5
RFC 1490 Multiprotocol interconnect over frame relay (obsoletes RFC 1294)

RFC 1541 Dynamic Host Configuration Protocol (DHCP)* *3Com passes DHCP requests but does not act as a client
RFC 1551 Novell IPX over various WAN media (IPX WAN)
RFC 1570 PPP LCP extensions
RFC 1593 APPN MIB definition
RFC 1634 IPX WAN version 2 (obsoletes RFC 1362)
RFC 1661 Point-to-Point Protocol (obsoletes RFCs 1171, 1331)
RFC 1717 PPP Multilink Protocol (MP)
RFC 1749 IEEE 802.5 station source routing MIB
RFC 1812 Router Requests

ISO/OSI Standards
IS 7498 Addendum 1 -Connectionless- mode transmission
IS 8208 X.25 packet level for DTEs
IS 8348 Addendum 2 - NSAP Addressing
IS 8473 Connectionless Network Protocol (CLNP)
IS 8802/2 Logical LinkControl (LLC)
IS 8802/3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IS 8802/5 Token Ring access method
IS 9542 End System to Intermediate System (ES-IS)
IS 10589 Intermediate System to End System (IS-ES)

AppleTalk Standards
Phase 2 Inside AppleTalk, Routing 2nd edition
Phase 1 Ethernet/FDDI as Bridging per the recommended practice of bridging agreed upon within
IEEE 802.1d

SMDS Standards
DXI 1991 MDS Interest 3.2 Group
TR-TSV- Bellcore
000772 Technical Reference for SIP level 3

ATM Standards
ATM Data Specification Exchange version 1.0, Interface August 4, (DXI)
l993 (mode 1A)
ATM User Specification Network versions 3.0 and 3.1 Interface (UNI)
LAN emulation Specification over ATM version 1.0

Appendix D - Computer Specification

Silicon Graphics Challenge XL

Technical Specifications

Processor Data

MIPS R10000 64-bit RISC CPU

Quantity
: 2 to 36

Primary Cache
: 32KB on-chip instruction cache 32KB on-chip data cache

Secondary Cache
: 1 or 4MB* secondary cache per processor

Systems Bus

Bandwidth
: 1.2GB/sec, sustained parity protected

Size 256-bit wide data path 40-bit wide physical address path

Memory subsystem

Physical Memory
: 64MB to 16GB, ECC protected

Interleaving
: 1,2,4, or 8-way

High-Speed I/O Subsystem

Bus Type
: SGI HIO bus (320MB/sec)

Bandwidth
: 160MB/sec per HIO slot

No. of Buses
: 1 to 6

No. of HIO Slots
: 2 to 12

Industry Standard I/O Subsytem

Bus Type
: VME64 bus

Bandwidth
: 50MB/sec per VME-64 bus

No. of VME Buses
: 1-5

No. of VME slots
: 5-25

Mass Storage

Interfaces
: Up to 42 SCSI-2 channels

Protocols
: SCSI-2, FAST/WIDE, single-ended or differential

Max. Bandwidth
: 20MB/sec per channel

Device Capacity
: 2GB, 4.3GB, or 9.1GB*, formatted

External Storage

Vault XL
: 873.6GB max per unit

Max. configuration
: 5.6TB max non-RAID 17.4TB max RAID

Removable Media

SCSI Devices
: CD-ROM, DAT, 8mm tape drive, 1/4" cartridge tape DLT

Communications

Integrated Serial I/O
: Up to 4 serial ports @ 9600 baud Ethernet, SCSI-2

Integrated Parallel I/O
: Up to 4 parallel ports

VME Controllers

Ethernet, FDDI, Token Ring, X.25, 100Base-T

SGI HIO Controllers

Dual FDDI, HiPPI, SCSI-2, 8-port Ethernet ATM

Dimensions & Weights

Dimensions

Height: 62.3"
Width: 27"
Depth: 48"

Net Weight

400 lbs (181 kg)

Vault XL Dimensions

Height: 62.3"
Width 27"
Depth: 48"

Environmental (Non-operating)

Temperature

-20 to +60 C

Humidity

10% to 95% non-condensing

Altitude

40,000 MSL

Environmental (Operating)

Temperature

+5 to +35 C

Humidity

10% to 80% non-condensing

Altitude

10,000 MSL

Noise

65 dBA

Electrical & Power

Voltage - Standard

208-230 VAC 1 Phase

Voltage - Optional

208 VAC 3 phase U.S.

Voltage - Optional

400 VAC 3 phase Europe

Frequency

50/60 Hz

Heat Dissipation

16,000 BTU/hr, max (1 Phase) 24,000 BTU/hr, max (3 phase)

Electrical Service

220 VAC @ 30A (1 phase) 208 VAC @30A (3 phase, 4 wire) 400 VAC @15A (3 Phase, 5 wire)

Service Type

IEC-309

Software

System Software

IRIX(TM) 6.2, X/Open XPG4 BASE 95,IEEE POSIX 1003.2, FIPS 151-1, SVR4 UNIX(TM) System V, 4.3 BSD extensions, MIPS ABI, SVID Issue 3, X11R6 Window System, Motif(TM) Window Manager 1.2, IRIS GL(TM)

Compilers

ANSI C, C++, Fortran77, Ada, Pascal, Power C Accelerator (PCA), Power Fortran Accelerator (PFA)

Networking

TCP/IP, NFS(TM) DECnet(TM), LAT(TM) IBM 3270(TM), IBM 5080(TM) , SNA3270(TM), SNA3770(TM), SNA LU6.2, NetVisualyzer(TM) SPECTRUM(TM) SNMP management, SNMP MIB,

Server Software

IRIS Networker(TM) XFS 64-bit journaled filesystem with guaranteed rate I/O IRIX Pro Systems Management Toolbox, Performance Co-Pilot(TM) system and network performance monitoring software

Regulatory Agency Approvals

Electromagnetic

FCC Class A

Emission

Canada DOC. Class A, CISPR 22 Class A, Germany VDE Class A, VCCI Class 1

Product Safety

UL 1950
CSA 22.2 (#950)
IEC 950
EN 60-950
Class 1 SELV

Ergonomic/Health

Germany ZH618

Origin2000TM

Technical Specifications

PROCESSOR DATA

Microprocessor
MIPS RISC R10000 64-bit CPU

Primary caches
32KB two-way set-associative on-chip instruction cache
32KB two-way set-associative on-chip data cache

Secondary cache
1MB or 4MB two-way set-associative cache per CPU

NODE CARD

CPU capacity
1 to 2 R10000 CPUs

Memory
64MB to 4GB ECC protection

Capacity
SDRAM

HW cache coherency
Yes

Interleaving
4-way per node card

Memory bandwidth
Up to 700MB/sec sustained
Up to 780MB/sec peak

DESKSIDE SYSTEM OR RACK MODULE

Processors
1 to 4 node cards, 1 to 8 CPUs

I/O bandwidth
5.12GB/sec sustained
Up to 6.2GB/sec peak

I/O boards
12 XIO™ or
11 XIO and 3 PCI 32- or 64-bit

Internal peripherals
5 3.5-inch Ultra SCSI devices
1 5.25-inch SCSI device

Independent power
Yes

Redundant power
Optional*

Redundant cooling
Yes

MAXIMUM RACK SYSTEM

Processors
1 to 64 node cards, 2 to 128 CPUs
I/O bandwidth
82GB/sec sustained, 102GB/sec peak
I/O boards
192 XIO or
184 XIO and 24 PCI 32- or 64-bit
Internal peripherals
128 3.5-inch Ultra SCSI devices,
16 5.25-inch SCSI devices
Independent power
Yes
Redundant power
Optional*
Redundant cooling
Yes

STORAGE I/O DEVICES

XIO cards supported
Base I/O includes internal SE Ultra SCSI, external SE Ultra SCSI, 100Base-TX, two 460kbps serial ports
4-port Ultra SCSI (3 differential, 1 SE or differential)
2-port Fibre Channel (copper or fiber)
PCI-64 cards supported
2-port Fibre Channel

NETWORK I/O DEVICES

XIO cards supported
Base I/O includes internal SE Ultra SCSI, external SE Ultra SCSI, 100Base-TX, 2 460kbps serial ports
4-port 100Base-TX and 6 460kbps serial ports
4-port ATM OC3
DVS (Serial CCIR601 digital video)
HIPPI-Serial (200MB/sec)
PCI-64 cards supported
Dual attached FDDI
single attached FDDI
UTP FDDI
Token Ring

ISDN
high-speed synchronous serial

I/O EXPANSION DEVICES

XIO to internal PCI (3 slots) adapter
XIO to external PCI adapter*
XIO to external VME adapter

MASS STORAGE

Interfaces
Ultra SCSI and Fibre Channel
Max. bandwidth
40MB/sec Ultra SCSI
100MB/sec Fibre Channel
Device capacity
4.5GB, 9.1GB
External storage
Rack-mount vaults
6 3.5-inch devices Ultra SCSI
10 3.5-inch devices Fibre Channel
RAID
Fast/Wide SCSI rack
(80 3.5-inch devices)
Maximum configuration
14.5TB per module (Fibre Channel)
3.5TB per module (Ultra SCSI)
13.5TB per module (Ultra SCSI RAID)

DIMENSIONS AND WEIGHTS

Deskside system
25.5" H, 23" D, 21" W (65cm H, 58cm D, 53cm W)
215 pounds (98kg)
Rack system
73" H, 40" D, 28" W (185cm H, 102cm D, 71cm W)
700 pounds (317kg)

Note: weights assume that modules are fully configured with processors, I/O, and peripherals.

ENVIRONMENTAL (NON-OPERATING)

Temperature
-20° to +60° C
Humidity

10% to 95% non-condensing

Altitude

40,000 MSL

SYSTEM BANDWIDTH

System bus bandwidth as measured by bisection bandwidth sustained (peak)

System size (CPUs)	Bisection bandwidth without Xpress links	Bisection bandwidth with Xpress links
8	1.28GB/sec, (1.)	2.56GB/sec, (3.2) (Star Router)
16	2.56GB/sec, (3.2)	5.12GB/sec, (6.4)
32	5.12GB/sec, (6.4)	10.2GB/sec, (12.8)
64	10.2GB/sec, (12.8)	n/a
128	20.5GB/sec, (25.6)	n/a

ELECTRICAL AND POWER

Voltage (deskside)

110-220 VAC (configuration limits apply at 110 VAC)

Voltage (rack)

220 VAC single-phase

Frequency

50-60Hz

Heat/power

2,500 watts, dissipation 8,500 BTU/hr (deskside)
5,500 watts, dissipation 18,750 BTU/hr (rack)

Electrical service/type

NEMA 5-20, type 110VAC @ 20amp (deskside)
NEMA 6-20, 208VAC @ 20amp (deskside)
NEMA 6-30, 208VAC @ 30amp (rack)

SOFTWARE

System software

Cellular IRIX™

Networking

TCP/IP, NFS™ V2/V3, RSVP, DHCP, Bulk Data Service (BDSpro), NetVisualyzer™,
SNMP management, SNMP MIB, NIS/ONC+

Server software

XFS™ 64-bit journaled filesystem with guaranteed rate I/O, IRIS NetWorker™, Performance
Co-Pilot™ system and network performance monitoring software, System MIB (Provision),
Software Distribution (Propel)

Compilers

ANSI C, C++, Fortran 77, Ada, Pascal, Power C Accelerator (PCA), Power Fortran 77,
Fortran 90, Power Fortran 90

PC/Macintosh® integration

Syntax TotalNET Advance server, supports Windows® 95 and Windows NT® (SMB),
NetWare™, AppleShare® environments for PC and Macintosh

Security

Trusted IRIX™ B1 security, Commercial Security Pack (CSP)

Web server

Netscape™ Enterprise server

Dell

Technical Specifications

Microprocessor

Microprocessor type	3.3-V P54C Pentium® chip
Microprocessor speeds	75/50 MHz internal/external 90/60 MHz internal/external
Internal cache	8 KB instruction 8 KB data
Math coprocessor	internal
Microprocessor socket	ZIF

System Information

System chip set	VLSI 590
Data bus width	64 bits
Address bus width	32 bits
DMA channels	7
Timers	3
Interrupt levels	15
Flash BIOS EPROM	1 MB
Serial port UART	16550-compatible
Buffer	16 bytes

Expansion Bus

Bus type	ISA and PCI
ISA expansion slots	4 (1 connector shares a card-slot

	opening with a PCI connector)
PCI expansion slots	2 (1 connector shares a card-slot opening with an ISA connector)
ISA bus speed	8.25 MHz
PCI bus speed	33 MHz
PCI data transfer rate	70 MB/sec
PCI data width	32 bit

Memory

Architecture	72-pin, fast-page mode
Wait states	near zero
SIMM sockets	4
SIMM capacities	4, 8, 16, and 32 MB
SIMM type	32-bit, nonparity
Minimum RAM	8 MB
Maximum RAM	128 MB
Memory access time	
tRAC	70 ns fast-page mode
tCAC	20 ns
External cache 256 KB write-through	
Speed	15 ns
Type	nonremovable from system board
BIOS address	E0000 - FFFFFh

Drives

Externally accessible bays	(3) 5.25-inch bays
Internally accessible bays	(2) 3.5-inch bays

Ports

Externally accessible:	
Serial (DTE)	(2) 9-pin connectors (16550-compatible)
Parallel	(1) 25-hole connector (bidirectional) (AT-, PS/2-, ECP-compatible)
Video	(1) 15-hole connector
PS/2-style keyboard	(1) 6-pin mini-DIN
PS/2-compatible mouse	(1) 6-pin mini-DIN
Internally accessible:	
Primary IDE	40-pin connector (hard-disk drives only)
Secondary IDE	40-pin connector (IDE devices)

Video

Type	S3Trio64 (PCI)
Standard memory	1 MB
Upgradable	2 MB

Power

DC power supply:	
Wattage	145 W
Voltage	90 to 135 V at 60 Hz or 180 to 265 V at 50 Hz

Physical

Height	16.2 cm (6.4 inches)

Width	43.2 cm (17 inches)
Depth	42.2 cm (16.6 inches)
Weight	13.2 kg (29.1 lb)

Environmental

Temperature:	
Operating	10 to 35C (50 to 95F)
Storage	-40° to 65°C (-40° to 149°F)
Relative humidity	8% to 80% (noncondensing)
Vibration:	
Operating	0.25 G at 3 to 300 Hz for 15 minutes
Storage	0.5 G at 3 to 300 Hz for 15 minutes
Shock:	
Operating	5 G for 11 ms
Storage	20 G with a velocity change of 1397 mm/sec
Altitude:	
Operating	-16 to 3048 m (-50 to 10,000 ft)
Storage	-16 to 10,600 m (-50 to 35,000 ft)

Regulatory Notices

FCC (U.S. only)	Class B
IC (Canada)	Class B
CE	Class B
VCCI (Japan)	Class 1
Czech	Category B

Appendix E - Acronyms:

ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
COTS	Commercial Off-the-Shelf
CSB	Computer Services Branch
DAAC	Distributed Active Archive Center
DHF	Data Handling Facility
DMO	DHF Management Organization
EBnet	EOSDIS Backbone Network
ECS	EOSDIS Core System
EDC	EROS Data Center
FDDI	Fiber Distributed Data Interface
Gbyte	Gigabyte
GSC	Ground Station Controller
GSFC	Goddard Space Flight Center
IAS	Image Assessment System
ICD	Interface Control Document
LAN	Local Area Network
LGS	Landsat 7 Ground Station
LPS	Landsat 7 Processing System
L0R	Level Zero Reformatted
MCS	Monitor and Control System
MOC	Mission Operations Center
MODNET	Mission Operations and Data Systems Directorate (MODSD) Operational Development Network
NISN	NASA Integrated Support Network
NTP	Network Time Protocol
PTP	Programmable Telemetry Processor
SGI	Silicon Graphics, Incorporated
TBD	To Be Defined/Determined
TBS	To Be Specified
TDF	Tracking Data Formatter
UPS	Uninterruptible Power System
USGS	United States Geological Survey
WAN	Wide Area Network